اُردو زَبان میں اِنفارمیشن ٹیکنالوجی کا وَاحِد مُستند جریدہ

ماہنامہ

کمپیوٹنگ

فروری 2017ء

شمارہ نمبر 125

قیمت 80 روپے

پوسٹل رجسٹریشن نمبر MC- 1264



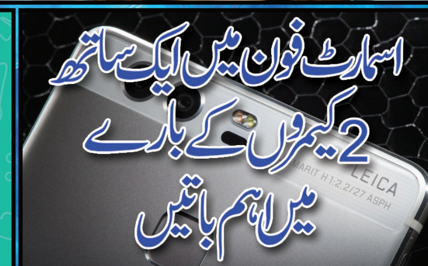












کیا آپ ...

ویب سائٹ بنوانا چاہتے ہیں یا موجودہ ویب سائٹ میں ترمیم چاہتے ہیں؟

اپنی ویب سائٹ کے لئے ہوسٹنگ ڈھونڈ رہے ہیں؟

اپنی ویب سائٹ کے لئے ڈومین نیم رجسٹر کروانا چاہتے ہیں؟

کوئی سافٹ ویئر بنوانا چاہتے ہیں؟

مائیکروسافٹ ونڈوز سمیت دیگر کوئی سافٹ ویئر خریدنا چاہتے ہیں؟

ہم سے بات کریں



مفت مشورے کے لئے کال کیجئے

0316 (ECRUSYS)

فہرست

شمارہ نمبر 125

جلد نمبر 10......شمارہ نمبر 5......فروری 2017ء

سرپرستِ اعلیٰ

گوہر رحمان

مدیر اعلیٰ

امانت علی گوہر

مدیر

علمدار حسین

مدیر سیکشن ٹیکنالوجی نیوز

رانا محمد امین اکبر

مجلسِ مشاورت

شبیر حسین قریشی، محبوب الٰہی مخمور، عمران احمد لاکھا (ایم فل)

قیمت فی شمارہ

80 روپے

زرسالانہ برائے پاکستان (رجسٹرڈ ڈاک)

825 روپے سالانہ

خط و کتابت کا پتا

پی او باکس نمبر 786، کراچی 74200

ٹیلی فون نمبر

0342 2507 857

دفتری اوقات

صبح 10 بجے تا سہ پہر چار بجے

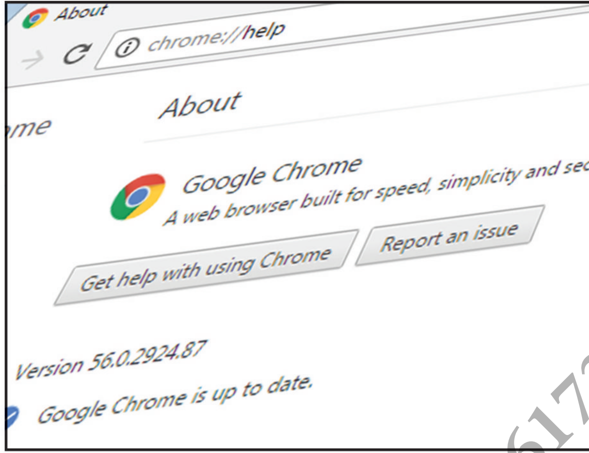
ای میل ایڈریس

crm@computingpk.com

پوسٹل رجسٹریشن

MC-1264

گوگل کروم اپ ڈیٹ کرلیں، ورنہ جی میل نہیں چلے گا



اگر آپ اب تک گوگل کروم براؤزر کے پرانے ورژن پر کام کر رہے ہیں، تو ہوشیار ہوجائیں۔ کیونکہ گوگل اب خطرے کی گھنٹی بجانے ہی والا ہے۔ 8 فروری کے بعد بھی اگر آپ گوگل کروم کا ورژن 53 یا اس سے پرانا استعمال کر رہے ہیں تو گوگل کی معروف ای میل سروس جی میل میں آپ کو وارننگ نظر آنا شروع ہوجائے گی کہ نئے ورژن پر اپ گریڈ ہوجائیں۔ اس لئے تکلیف سے بچنے کیلئے گوگل کروم کو فی الفور نئے ورژن پر اپ گریڈ کرلیں۔ کروم کے نئے ورژن میں کئی سکیورٹی اپ ڈیٹس شامل کی گئی ہیں تاکہ آپ محفوظ انداز میں انٹرنیٹ استعمال کرسکیں۔

اگر گوگل کروم آپ کا پسندیدہ ویب براؤزر ہے اور آپ اب تک مائیکروسافٹ ونڈوز ایکس پی اور ونڈوز وِستا پر کام کر رہے ہیں، تو آپ کا کام متاثر ہوسکتا ہے۔ کیونکہ گوگل کروم کے نئے ورژنز ان آپریٹنگ سسٹم پر نہیں چل پائیں گے۔ گوگل کروم کا ورژن 49 وہ آخری ورژن تھا جو ونڈوز ایکس پی اور ونڈوز وستا کے لئے دستیاب تھا۔

اپنی ایک بلاگ پوسٹ کے ذریعے گوگل نے بتایا کہ وہ صارفین جو گوگل کروم ورژن 53 یا اس سے پرانا ورژن استعمال کر رہے ہیں، ان کے پاس دسمبر 2017ء تک کا وقت ہے کہ وہ اپ گریڈ ہوجائیں۔ اس کے بعد جی میل کا جدید اور انٹرایکٹیو انٹرفیس ان کے لئے دستیاب نہیں ہوگا اور انہیں جی میل کا بیسک ایچ ٹی ایم ایل ورژن دکھائی دینا شروع ہوجائے گا۔ سال 2013ء میں گوگل نے کہا تھا کہ وہ ونڈوز ایکس پی پر گوگل کروم کی سپورٹ اپریل 2015ء تک جاری رہے گی، تاہم بعد میں اس نے 2015ء کے آخر تک تاریخ بڑھا دی تھی۔ پھر نومبر میں گوگل نے کہا کہ اب وہ ونڈوز ایکس پی، وستا اور میک OS X کے پرانے ورژن کو سپورٹ کرنا 2016ء میں بند کردے گا، جو اس نے کروم ورژن 49 کے ساتھ کیا بھی۔

نوٹ کرنے والی بات یہ ہے کہ گوگل کروم کے پرانے ورژن پر جی میل کا استعمال محفوظ نہیں اور جی میل میں متعارف کروائی گئی نئی سہولیات سے بھی فائدہ نہیں اٹھایا جاسکے گا۔ اس لئے یہ آپ کے مفاد میں ہے کہ گوگل کروم کا تازہ ترین ورژن انسٹال کرلیں۔ اس نئے ورژن کے بارے میں گوگل کا دعویٰ ہے کہ وہ ویب پیج لوڈ کرنے کی رفتار میں 28 فیصد تک کمی کرتا ہے اور یہ بہتری صرف ڈیسک ٹاپ نہیں بلکہ موبائل فون کے لئے دستیاب گوگل کروم میں بھی دیکھی جاسکے گی۔ گوگل کے مطابق اس ورژن میں Validation تکنیک استعمال کی گئی ہے جس میں گوگل کروم سرور سے پوچھتا ہے کہ اس کے پاس کیش (cashe) میں موجود فائلیں کیا ابھی تک قابل استعمال ہیں۔ اگر جواب ہاں میں ملتا ہے تو کروم وہ فائلیں سرور سے دوبارہ ڈاؤن لوڈ کرنے کے بجائے کیش میں سے لوڈ کرلیتا ہے۔

2018ء تک 16TB گنجائش والی ہارڈ ڈسک کا منصوبہ



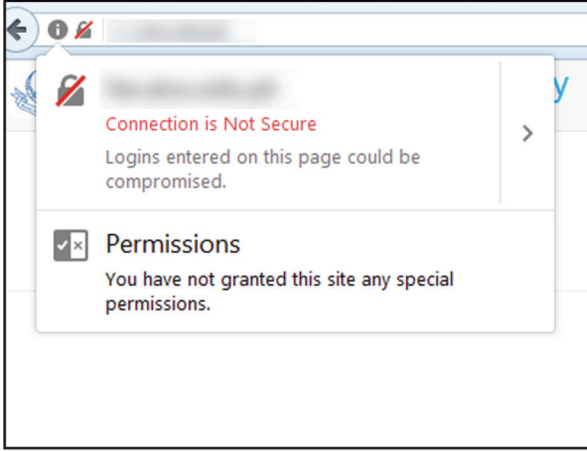
2002ء کی بات ہے جب ایک دوست نے بتایا کہ اس نے 40 جی بی کی ہارڈ ڈسک خریدی ہے۔ یہ سن کر منہ کھلا کا کھلا رہ جانا کوئی اچھنبے کی بات نہیں تھی کیوں کہ اس وقت لوگ 4 جی بی کی ہارڈ ڈرائیو کے ساتھ بھی ہنسی خوشی گزارا کر رہے تھے۔ اس 40 جی بی ہارڈ ڈرائیو کی قیمت اس سے بھی زیادہ منہ کھولنے والی تھی، یعنی بارہ ہزار روپے!

اگر آپ کمپیوٹر پروسیسرز کے بارے میں سطحی سی معلومات بھی رکھتے ہیں تو آپ کے علم میں مور کا قانون ضرور ہوگا۔ انٹل کے بانی گورڈن مور کے نام پر رکھے گئے اس قانون کے مطابق ہر اٹھارہ ماہ میں انٹی گریٹڈ سرکٹس (IC) میں ٹرانسسٹر کی تعداد دگنی ہوجاتی ہے۔ اس کا مطلب یہ نہیں کہ آپ کے پاس موجود پروسیسر کے ٹرانسسٹر خفیہ طور پر انڈے یا بچے دیتے ہیں جس کی وجہ سے ٹرانسسٹرز کی تعداد دگنی ہوجاتی ہے۔ بلکہ اس کا مطلب یہ ہے کہ آج اگر ایک ارب ٹرانسسٹرز والا پروسیسر دستیاب ہے تو اٹھارہ ماہ بعد ہم 2 ارب ٹرانسسٹرز والا پروسیسر بھی بنا چکے ہونگے۔ ایسا ہی ایک قانون ہارڈ ڈسک کے لئے بھی ہے۔ اسے کریڈر کا قانون کہا جاتا ہے اور اسے پیش کرنے والے صاحب ڈاکٹر مارک کریڈر سی گیٹ کارپوریشن کے سابق سینئر نائب صدر چیف ٹیکنالوجی آفیسر ہیں۔ 2005ء میں انہوں نے سائنٹیفک امریکن میں اپنے اس قانون کے متعلق مضمون تحریر کرتے ہوئے لکھا کہ مقناطیسی قرص (ڈسک) پر ڈیٹا محفوظ کرنے کی گنجائش میں زبردست اضافہ ہورہا ہے۔ یہ رفتار اٹھارہ ماہ میں ٹرانسسٹرز کی تعداد دگنی ہوجانے سے بہت زیادہ ہے۔ اس قانون یا صحیح الفاظ میں مشاہدے کی صداقت مشکوک ہے۔ تاہم اگر اس قانون کو مدنظر رکھا جائے تو 2020 تک ہارڈ ڈسک میں ڈیٹا محفوظ کرنے کی گنجائش 40 ٹیرابائٹس تک پہنچ جائے گی اور اس کی قیمت 40 ڈالر تک ہوگی۔

دوسری جانب مارک کریڈر کی کمپنی سی گیٹ ہارڈ ڈسک کی گنجائش بڑھانے میں جُتی ہوئی ہے۔ گزشتہ سال سی گیٹ نے ساڑھے تین انچ سائز میں 60 ٹیرابائٹس کی سالڈ اسٹیٹ ہارڈ ڈسک بنائی تھی۔ تاہم مقناطیسی قرص (ڈسک) والی ہارڈ ڈرائیو کی گنجائش اب بھی کافی کم ہے۔ دیکھا جائے تو سی گیٹ کی وجہ شہرت ہی اس کی مقناطیسی ڈسک والی ہارڈ ڈرائیوز ہیں کیونکہ سالڈ اسٹیٹ کے میدان میں سی گیٹ سے بڑے کھلاڑی پہلے ہی موجود ہیں۔ سی گیٹ نے ایک کانفرنس کے دوران اپنے مستقبل قریب کے منصوبوں کے بارے میں بتایا ہے۔ کمپنی چند سالوں میں ڈرائیو کی گنجائش کو بہت زیادہ بڑھا دے گی۔ اس وقت کمپنی کی سب سے زیادہ گنجائش والی ڈرائیو 10 ٹیرابائٹس کی ہے۔ لیکن کمپنی کا خیال ہے کہ اگلے تین سالوں میں وہ اسے دوگنا کردے گی۔ سی گیٹ 2018ء کے وسط تک 16 ٹیرابائٹس کی ڈرائیو متعارف کرائے گی۔ اس کے باوجود 2020ء تک 40 ٹیرابائٹس کی گنجائش تک پہنچنا بے حد مشکل نظر آرہا ہے۔

یونٹ کی فروخت کے حساب سے دیکھا جائے تو مقناطیسی ہارڈ ڈرائیو کی فروخت میں کافی کمی ہوئی ہے۔ اس کی وجہ سالڈ اسٹیٹ ہارڈ ڈرائیوز کا مارکیٹ میں اپنی جگہ مستحکم کرنا ہے۔ سی گیٹ کی فروخت صرف پچھلے سال کے مقابلے میں ہی 10 فیصد کم ہوگئی ہے۔ سی گیٹ کے لیے زیادہ گنجائش والی ہارڈ ڈرائیو کی بڑے پیمانے پر فراہمی کے کئی مالی فوائد بھی ہیں۔ مثلاً نگرانی کے آلات کے لئے بڑی گنجائش والی اسٹوریج ڈیوائس بنانا سی گیٹ کے لئے بے حد فائدہ مند ثابت ہوا ہے۔

غیر محفوظ ویب سائٹس کے خلاف کروم اور فائر فاکس کا محاذ



غیر محفوظ ویب پیجز کے حوالے سے ایک جنگ شروع ہوچکی ہے اور اس حوالے سے پہلا وار موزیلا نے کیا ہے۔ حال ہی میں موزیلا نے فائر فاکس 51 کو عام صارفین کے لیے جاری کیا ہے۔ نئے ورژن میں موزیلا نے صارفین کو غیر محفوظ ویب سائٹس سے خبردار کرنے کا فیچر بھی شامل کیا ہے۔ اب فائر فاکس صارفین ایسی تمام ویب سائٹس سے خبردار ہوسکیں گے، جن پر لاگ ان کرنا اُن کے لیے غیر محفوظ ہوگا۔ یعنی ایسی تمام ویب سائٹ جو HTTPS کی بجائے HTTP پروٹوکول استعمال کر رہی ہونگی، فائر فاکس صارفین کو اُن کے بارے میں خبردار کر دے گا۔ گوگل کروم بھی موزیلا کے نقش قدم پر چلتے ہوئے یہ 31 جنوری کو ریلیز ہونے والے اپنے ورژن 56 میں غیر محفوظ ویب سائٹس کے خلاف خبردار کرنا شروع کر چکا ہے۔

HTTP پروٹوکول صارف اور ویب سائٹ کے درمیان ایک ایسا کنکشن بناتا ہے جو انکرپٹ (رمزشدہ) نہیں ہوتا ہے۔ اس لئے اس پروٹوکول کو غیر محفوظ مانا جاتا ہے اور اسے استعمال کرنے والی ویب سائٹس پر اپنی نجی معلومات مثلاً پاس ورڈ یا کریڈٹ کارڈ نمبر فراہم کرنا خطرناک ہوسکتا ہے۔ HTTP پروٹوکول کے ذریعے صارف کے کمپیوٹر سے کسی سرور کی جانب بھیجا گیا ڈیٹا راستے میں ہی اُچکا جاسکتا ہے۔ چونکہ وہ ڈیٹا انکرپٹ نہیں ہوتا، اس لئے ڈیٹا کو اُچکنا ہی کافی ہوتا ہے۔ ڈیٹا کی حفاظت چونکہ ایک حساس مسئلہ ہے، اس لئے تمام اہم ویب سائٹس HTTPS پروٹوکول استعمال کرتی ہیں۔ یہ محفوظ پروٹوکول ہے اور اس میں سرور اور صارف کے درمیان ہونے والے ڈیٹا کی منتقلی مکمل طور پر رمزشدہ ہوتی ہے۔ اس لئے اگر راستے میں کوئی ہیکر ڈیٹا اُچک بھی لے تو وہ ڈیٹا اس کے کسی کام کا نہیں ہوگا۔ تاہم اب بھی کروڑوں ویب سائٹس ایسی ہیں جو HTTP ہی پر اکتفا کئے ہوئے ہیں۔ ایسی ویب سائٹس کے لئے گوگل کروم اور موزیلا نے محاذ بنالیا ہے۔

فائر فاکس کے ایسے صارفین جنہوں نے اپنا ویب براؤزر حال ہی میں اپ ڈیٹ کیا ہو، انہیں ایڈریس بار کے بائیں جانب ایک تالے کا آئیکون نظر آئے گا۔ غیر محفوظ ویب سائٹس پر اس کے اوپر ایک سرخ رنگ کی ترچھی لائن نظر آئے گی، جس کا مطلب ہوگا کہ صارفین اس ویب سائٹ پر اپنا ڈیٹا ڈالتے ہوئے احتیاط کریں کیونکہ ان کا ڈیٹا چرایا جاسکتا ہے۔ اس تالے کے آئیکون پر کلک کرنے سے صارفین پیج کے محفوظ یا غیر محفوظ ہونے کے بارے میں مزید معلومات دیکھ سکتے ہیں۔ خاص طور پر ایسے صفحات جہاں لاگ ان معلومات یا صارف سے کچھ ٹائپ کرنے کو کہا جارہا ہو، موزیلا فائر فاکس خاص طور پر صارف کو خبردار کرے گا۔

کروم سے اس حوالے سے تھوڑا سا مختلف طریقہ اختیار کیا ہے۔ کروم میں صارفین ترچھی لکیر والے تالے کے نشان کی بجائے ایڈریس بار کے بائیں جانب انفارمیشن آئیکون اور اس کے ساتھ Not Secure یا Secure لکھا ہوا دیکھیں گے۔ کروم صرف اس صورت میں صارف کو خبردار کرے گا جب وہ کسی ایسی ویب سائٹ پر ہوگا جہاں صارف سے اس کا ڈیٹا مثلاً یوزنیم، پاس ورڈ وغیرہ طلب کیا جارہا ہے۔

سب سے زیادہ استعمال کئے جانے والے ویب براؤزرز کی جانب سے یہ قدم اٹھانا ویب سائٹ مالکان کو مجبور کرے گا کہ وہ اپنی ویب سائٹس محفوظ پروٹوکول پر منتقل کریں ورنہ ان کے صارفین ان کی ویب سائٹ پر آنا بند کر سکتے ہیں۔

وٹس ایپ برائے آئی فون میں آف لائن پیغامات کی اجازت



اب وہ دن گئے جب ایپل پر وٹس ایپ میسج بھیجنے کے لیے انٹرنیٹ کنکشن لازمی ہوتا تھا۔ ایک نئے فیچر سے آئی فون پر وٹس ایپ استعمال کرنے والے میسیجز کو آف لائن رہتے ہوئے بھی بھیج سکیں گے۔ اینڈرائیڈ صارفین کے لئے یہ خاصی حیرت کی بات ہوگی کہ ایپل آئی فون کے لئے دستیاب وٹس ایپ میں صارفین کسی کو پیغام بھیجنا چاہیں تو ان کا آن لائن ہونا ضروری ہے۔

نئے فیچر کی بدولت ایپل صارفین کے آف لائن پیغامات کو ایپلی کیشن اپنے پاس محفوظ کرلے گی اور جیسے ہی فون انٹرنیٹ سے جڑے گا، پیغامات کو ان کی منزل کی جانب روانہ کردیا جائے گا۔ اس سہولت سے فائدہ اٹھانے کے لئے ایپل صارفین کو وٹس ایپ کا تازہ ترین ورژن نصب کرنا ہوگا۔ اینڈرائیڈ صارفین تو پہلے ہی اس سہولت سے مستفید ہورہے ہیں۔

ایپلی کیشن کی تازہ ترین اپ ڈیٹ سے صارفین ایک ساتھ 30 تصاویر یا ویڈیوز بھیج سکتے ہیں۔ اس سے پہلے یہ حد 10 تصاویر یا ویڈیوز کی تھی۔ ایک نیا فیچر Storage Usage ڈسک اسپیس خالی کرنے کے لئے معاونت کرے گا۔

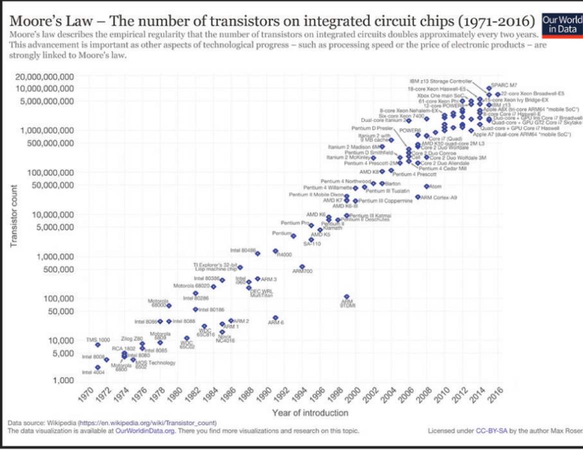
فیس بک پر زیادہ پوسٹس کی وجہ سے صحت ہوسکتی ہے خراب

فیس بک پر بہت زیادہ اسٹیٹس اپ ڈیٹ کرنا اور دوسروں کی پوسٹس لائک کرنا آپ کی ذہنی اور جسمانی صحت کے لئے خطرناک ہوسکتا ہے۔ ایک نئی تحقیق میں یہ بات دریافت ہوئی ہے۔ سان ڈیاگو میں واقع یونیورسٹی آف کیلی فورنیا کی اسسٹنٹ پروفیسر ہولی شاکیا (Holly Shakya) اور ان کے ساتھیوں نے 5200 لوگوں کے ڈیٹا کی جانچ کرکے یہ نتیجہ اخذ کیا۔

تحقیق میں شامل لوگوں کی اوسط عمر 48 سال تھی۔ نمونے تین مختلف وقت کے لئے گئے۔ تجربے میں شامل شرکاء کو روزمرہ جس طرح وہ فیس بک استعمال کرتے ہیں، استعمال کرنے کی اجازت دی گئی لیکن اس دوران ان کی کڑی نگرانی بھی کی گئی۔ ان کی فیس بک سرگرمیوں پر نظر رکھنے کے علاوہ ماہرین نے اس دوران ان کی صحت پر بھی خاص نظر رکھی اور مختلف آزمائشیں کرتے رہے۔

ماہرین نے یہ نتیجہ اخذ کیا کہ جن لوگوں نے دوسروں کی پوسٹس بہت زیادہ لائک کیں، ان کی صحت زیادہ خراب تھی۔ ریسرچرز نے یہ بھی جانا کہ جو لوگ اپنا فیس بک اسٹیٹس زیادہ اپ ڈیٹ کرتے تھے، ان کی ذہنی صحت کی حالت عام طور پر کم اسٹیٹس اپ ڈیٹ کرنے والوں کے مقابلے زیادہ خراب تھی۔ ریسرچرز کے یہ نتائج لائیو سائنس میں شائع ہوئے ہیں۔

انٹل پھر جُت گیا مور کا قانون بچانے کے لئے



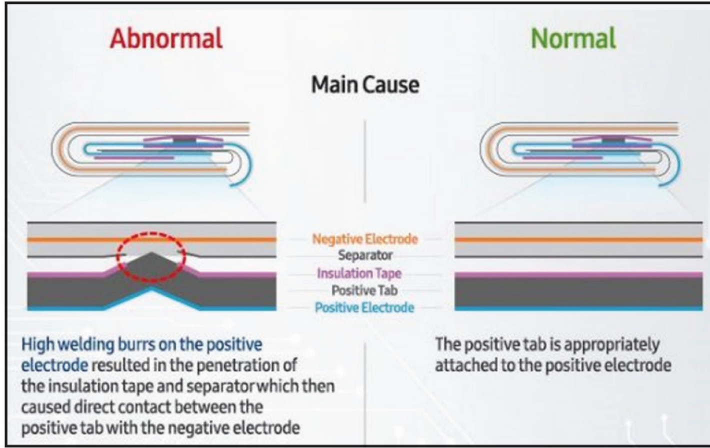
انٹل نے مور کے قانون کو بچانے کے لئے 7 نینومیٹر فیبری کیشن پروسس کا ایک پائلٹ (آزمائشی) پلانٹ لگانے کی تیاری شروع کردی ہے۔ کمپنی نے اس پلانٹ سے متعلق اعلان اپنے منافع اور کمائی کے اعلانات کے ساتھ ہی کیا ہے۔ کئی دہائیوں تک مور کے قانون نے انٹل کی پتلے ترین، تیز رفتار اور کفایت شعار پروسیسر بنانے میں رہنمائی کی ہے۔ اسی وجہ سے تیز رفتار کمپیوٹر، طویل وقت بیٹری پر چلنے کے قابل پتلے لیپ ٹاپ اور موبائل بنانا ممکن ہوسکا ہے۔

مور کے قانون کے ساتھ ایک بڑا مسئلہ ہے جس کا تذکرہ ماضی میں ہم کئی بار کر چکے ہیں۔ مور کا قانون (یا مشاہدہ) یہ کہتا ہے کہ انسان ہر اٹھارہ ماہ بعد ٹرانسسٹر کی تعداد دوگنی کرنے کے قابل ہوجائیں گے۔ گزشتہ کئی دہائیوں سے یہ قانون اپنی افادیت ثابت کرتا آیا ہے۔ 1971ء میں جب انٹل نے Intel 4004 مائیکرو پروسیسر نے پیش کیا تھا، اس پروسیسر کو 10000 نینومیٹر فیبری کیشن پروسس پر تیار کیا گیا تھا اور اس میں ٹرانسسٹرز کی تعداد 2300 تھی۔ سال 2000ء میں انٹل نے جس پینٹیئم فور پروسیسر کا اجراء کیا، اسے 180 نینومیٹر پروسس پر بنایا گیا اور اس میں چار کروڑ بیس لاکھ ٹرانسسٹر تھے۔ آج صورت حال یہ ہے کہ 22 کور پر مشتمل انٹل زیون Broadwell E5 پروسیسر میں سات ارب بیس کروڑ ٹرانسسٹر نصب ہیں اور اسے 14 نینومیٹر پروسس پر بنایا گیا ہے۔ یہ بات بھی دلچسپی سے پڑھی جائے گی کہ این ویڈیا GP100 Pascal گرافیکل پروسسنگ یونٹ میں ہی 15 ارب 30 کروڑ ٹرانسسٹر لگے ہوئے ہیں اور اسے 16 نینومیٹر پروسس پر تیار کیا گیا ہے۔ ان اعداد وشمار کی روشنی میں اندازہ لگایا جاسکتا ہے کہ ٹرانسسٹرز کی تعداد کا بڑا انحصار اس بات پر ہے کہ انہیں کتنے نینومیٹر فیبری کیشن پروسس پر بنایا گیا ہے۔ آسان زبان میں بیان کیا جائے تو فیبری کیشن پروسس کا مطلب ٹرانسسٹر کا سائز ہوتا ہے۔ 14 نینومیٹر فیبری کیشن پروسس کا مطلب ہے کہ اس پروسس سے بننے والے پروسیسر میں ٹرانسسٹر کا سائز 14 نینومیٹر ہوگا۔ مور کے قانون کے ساتھ اب دقت یہ ہے کہ ہم ٹرانسسٹر کو اتنا چھوٹا کر چکے ہیں کہ اسے مزید چھوٹا کرنا اب روایتی ٹیکنالوجی کے لئے ممکن نہیں رہا۔ اس لئے بعض ماہرین کا خیال ہے کہ مور کا قانون بھی اب اپنی افادیت کھو چکا ہے۔ دوسری جانب انٹل کا کہنا ہے کہ ایسا نہیں ہے۔ انٹل کوشش کررہا ہے کہ اپنے پرانے مشاہدات کی روشنی چپ ٹیکنالوجی کو آگے بڑھائے۔

انٹل کا پائلٹ پلانٹ 7 نینومیٹر مائیکروچپس تیار کرنے کے تجربات کرے گا اور پتا لگایا جائے گا کہ اس پروسس پر کس طرح اربوں کی تعداد میں مائیکروچپس بنائی جاسکتی ہیں۔ تجربات کے آغاز سے تجارتی پیمانے پر تیاری میں خاصا وقت درکار رہتا ہے۔ اس لئے 7 نینومیٹر پروسس پر تیار کی گئی مائیکروچپس کی دستیابی اگلے چند سالوں کے دوران ممکن نہیں۔ کوئی بھی فیبری کیشن پلانٹ لگانا آسان کام نہیں۔ اس کے لئے اربوں ڈالر کی سرمایہ کاری درکار رہوتی ہے۔ اس پائلٹ پلانٹ کو انٹل کی جانب سے اربوں ڈالر کی سرمایہ کاری کی جانب پہلا قدم سمجھنا چاہئے۔

انٹل کی تازہ ترین چپ جس کا تعلق Kaby Lake (کوڈ نیم) سیریز سے ہے، کو 14 نینومیٹر پروسس پر بنایا گیا ہے۔ کمپنی جلد ہی Cannonlake سیریز کے پروسیسر پیش کرنے والی ہے جنہیں 10 نینومیٹر پروسیسر پر بنایا گیا ہے۔ ان چپس کو 2017ء میں ہی محدود تعداد میں فروخت کے لئے پیش کردیا جائے گا۔

سام سنگ نے نوٹ 7 کی بیٹری سے متعلق اپنی تحقیقات پیش کردیں

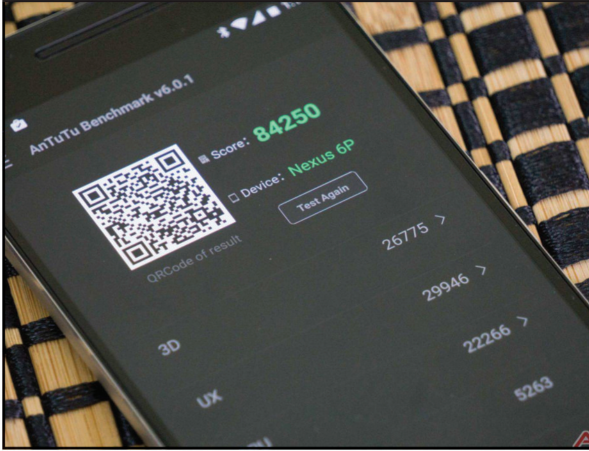


جب سے سام سنگ نے گلیکسی نوٹ 7 کو واپس منگوا کر دوبارہ جاری کیا اور پھر دوسری بار واپس منگوایا تب سے ہی لوگوں کے ذہنوں میں ایک ہی سوال ہے کہ آخر نوٹ 7 کے ساتھ ہوا کیا تھا، جس نے فون کو ختم کر دیا۔ اس حوالے سے چند سازشی نظریات بھی گردش میں رہے جن کے مطابق ایپل نے میڈیا کو پیسے دے کر فون میں آگ لگنے کی جعلی خبریں چلوائیں۔ دوسری وجوہ میں بیٹری کی خرابی کا ذکر تھا، جس کا پہلی بار بھی پتا نہ چل سکا اور دوسری بار بھی یہ وجہ شناخت نہ ہو سکی۔ اچھی بات یہ ہے کہ سام سنگ نے بھی نوٹ 7 کی خرابی کو سنجیدہ لیا اور اس حوالے سے خود بھی تحقیقات کیں اور دیگر کمپنیوں سے بھی تحقیقات کرائیں۔ سام سنگ کی تحقیقات میں بتایا گیا کہ نوٹ 7 میں ایک نہیں دو خرابیاں تھیں، جس نے نوٹ 7 سیریز کو ہی ختم کر دیا۔

سام سنگ نے پتا لگایا کہ بیٹری کے کونوں میں ایک ایسا نقص ہے جس کی وجہ سے بیٹری کے برقیرے (الیکٹروڈ) مڑ کر ایک دوسرے کے ساتھ مل سکتے ہیں اور بیٹری میں ہی شارٹ سرکٹ واقع ہو سکتا ہے۔ ابتداء میں جن بیٹریوں میں آگ لگی، اس کی وجہ یہی نقص تھا۔ سام سنگ نے اس نقص کا پتا لگا کر ایسی بیٹریوں والے فون فوراً واپس منگوا لئے تھے۔ گلیکسی نوٹ 7 کے لئے سام سنگ نے دو ذرائع سے بیٹری حاصل کر کے اس میں استعمال کیں۔ جب معلوم ہوا کہ ایک کمپنی کے بیٹری کے ڈیزائن میں خرابی ہے تو سام سنگ نے دوسری کمپنی سے بیٹریاں بنوانا شروع کر دیں۔ لیکن دوسری کمپنی کی بیٹریوں میں ویلڈنگ کی خرابی مسئلہ بن گئی۔ ناقص ویلڈنگ کی وجہ سے مثبت برقیرے میں کھردرا پن یا دوسرے الفاظ میں ابھار پیدا ہو گیا جو دبنے پر مثبت اور منفی برقیرے کو الگ رکھنے والی تہہ کو چیرتا ہوا منفی برقیرے تک پہنچ سکتا ہے۔ یوں بیٹری میں شارٹ سرکٹ ہو جاتا ہے۔ سام سنگ نے یہ بھی پتا لگایا کہ کچھ بیٹریوں میں انسولیشن ٹیپ جو منفی اور مثبت برقیرے کو الگ رکھتی ہے، موجود ہی نہیں تھی۔ ان نقائص کی وجہ سے سام سنگ دوسری بار بھیجے گئے نوٹ 7 کو پھر واپس منگوانے پر مجبور ہو گیا۔ چونکہ دونوں نقائص کا نتیجہ بیٹری میں آگ لگنے کی صورت میں نکلا، اس لئے لوگ سمجھے کہ سام سنگ نے مسئلہ حل کئے بغیر نوٹ 7 دوبارہ پیش کر دیا۔ حالانکہ پہلے اور دوسرے نقص میں خاصا فرق ہے۔

سام سنگ نے نوٹ 7 کی ناکامی کی تحقیقات 700 اسٹاف ممبران اور تین اضافی لیبارٹریوں UL، Exponent اور TUV Rheinland کے ساتھ کی۔ ٹیم نے 2 لاکھ اسمارٹ فون اور 30 ہزار بیٹریوں کی جانچ پڑتال کے بعد نتائج مرتب کئے۔ تحقیقات سے پتا چلا کہ گلیکسی نوٹ 7 کے ڈیزائن، اس کے چارجنگ سسٹم یا بیٹری پروگرامنگ میں کوئی خرابی نہیں تھی۔ اصل خرابی شارٹ سرکٹ کی تھی۔ اسی خرابی کی وجہ سے فون دوبار واپس منگوایا گیا۔ سام سنگ کی اپنی جلد بازی کو نظر انداز نہیں کیا جا سکتا۔ جب تک سام سنگ اپنے مرکزی بیٹری سپلائر کے ساتھ کام کرتا رہا، اسے کوئی مسئلہ درپیش نہیں آیا۔ لیکن کم وقت میں زیادہ سے زیادہ نوٹ سیون کی تیاری کے لئے جب اس نے بیٹری بنانے والے دوسرے ادارے کی خدمات حاصل کیں تو مسائل پیدا ہوئے۔ اگلے چند ہفتوں میں سام سنگ گلیکسی ایس 8 لانچ کر دے گا۔ اس کے بعد گرما میں گلیکسی نوٹ 8 لانچ کیا جائے گا۔ اب دیکھنا یہ ہے کہ آیا سام سنگ گلیکسی نوٹ کا برانڈ نیم ہی استعمال کرتا ہے یا اسے بھی تبدیل کرتا ہے۔

وَن پلس اور "مے یُو" کی بنچ مارک میں ہیرا پھیری پکڑی گئی



بینچ مارکنگ کسی ہارڈ ویئر کی کارکردگی جانچنے کے لئے کیا جانے والا ٹیسٹ ہے۔ اگر آپ LG جی 2 اور LG جی 3 کی بینچ مارکنگ کریں تو ایل جی جی تھری کا اسکور آپ کو زیادہ نظر آئے گا کیونکہ اس میں بہتر ہارڈ ویئر نصب ہے۔ اسمارٹ فونز کے شوقین بہت سے لوگ بینچ مارک اسکور دیکھ کر ہی کسی فون کو خریدنے کا فیصلہ کرتے ہیں۔ عام لوگوں کے لئے شاید بینچ مارکنگ زیادہ اہم نہ ہو، لیکن بہتر ہارڈ ویئر کے خواہش مند لوگ بینچ مارک اسکور پر خاص نظر رکھتے ہیں۔

لوگوں کی اسی کمزوری کا فائدہ اٹھاتے ہوئے ماضی میں کئی کمپنیاں بینچ مارک اسکور میں ہیرا پھیری کرتی پکڑی گئی ہیں تا کہ ان کے اسمارٹ فونز کا شاندار اسکور صارفین کو متاثر کر سکے۔ ان میں تمام ہی نامور کمپنیاں شامل ہیں۔ تاہم پکڑے جانے پر انہوں نے یہ کام بند کر دیا۔ اب تازہ خبر یہ ہے کہ OnePlus اور Meizu (دونوں چینی کمپنیاں ہیں) بینچ مارک میں ہیرا پھیری کرتی پائی گئی ہیں۔

بینچ مارکنگ ایپلی کیشنز اسمارٹ فون کی پروسیسنگ کی طاقت کو جانچ کر کے اس کے حساب سے اسکور دیتی ہیں۔ اس اسکور کی بنیاد پر اسمارٹ فونز کی درجہ بندی کی جاتی ہے۔ اگر آپ آپ کمپیوٹر یا لیپ ٹاپ پر ونڈوز سیون یا اس سے بہتر آپریٹنگ سسٹم استعمال کرتے ہیں تو سسٹم پراپرٹیز میں آپ کو سسٹم ریٹنگ نظر آئے گی۔ مائیکروسافٹ اسے ونڈوز ایکسپیرینس انڈیکس کہتا ہے۔ یہ بھی بینچ مارک کی ایک مثال ہے جس میں مائیکروسافٹ ونڈوز آپ کے کمپیوٹر/ لیپ ٹاپ میں نصب ہارڈ ویئر کی طاقت و کارکردگی کے مطابق اسکور دیتا ہے۔ یہ اسکور جتنا زیادہ ہوگا، ہارڈ ویئر اتنا ہی جدید/ بہتر تصور کیا جائے گا۔

اطلاعات کے مطابق وَن پلس تھری ٹی اور Meizu Pro 6 کو اس طرح سے تبدیل کیا گیا ہے کہ وہ بینچ مارکنگ ایپلی کیشن میں حقیقی اسکور کے مقابلے میں زیادہ اسکور ظاہر کرتے ہیں۔ وَن پلس نے اس غلطی کو تسلیم کرتے ہوئے اس جعل سازی کو دور کرنے کا وعدہ کیا ہے لیکن Meizu کی جانب سے فی الحال خاموشی ہے۔

ماضی میں سام سنگ اور ایچ ٹی سی سمیت کئی کمپنیوں پر ایسے الزامات لگتے رہیں کہ وہ دھوکے سے اپنا بینچ مارک اسکور زیادہ دکھاتی ہیں۔ جب اس بات کا انکشاف ہوا تھا تو سخت تنقید کے بعد کمپنیوں کو اس حرکت سے باز آنا پڑا تھا۔ وَن پلس کی جعل سازی کے بارے میں XDA ڈیولپرز کا دعویٰ ہے کہ انہوں نے غلط طریقے سے بینچ مارکنگ اسکور میں معمولی اضافہ کیا۔ اس معمولی اضافے کے لئے غلط طریقہ اختیار کرنے پر سوال کھڑے ہو رہے ہیں۔ وَن پلس نے البتہ یہ یقین دہانی کروائی ہے کہ OxygenOS کی اگلی اپ ڈیٹ میں اس مسئلے کو حل کر دیا جائے گا اور انہوں نے بنچ مارک میں ہیرا پھیری بھاری بھرکم ایپلی کیشنز اور ویڈیوز گیمز میں صارف کو بہتر تجربہ دینے کے لئے کی۔

مے یُو پرو 6 پلس کے بارے میں انکشاف کیا گیا ہے کہ جیسے ہی اس پر بینچ مارکنگ ایپلی کیشن کو چلایا جاتا ہے تو وہ نارمل موڈ سے پرفارمنس موڈ میں آجاتا ہے۔ پرفارمنس موڈ میں پروسیسر اپنی پوری قوت کے ساتھ چلنا شروع کر دیتا ہے۔ یوں اس کا اسکور بڑھ جاتا ہے۔ موبائل فون پروسیسر اپنی پوری قوت سے چلیں تو بہت جلد گرم ہو کر دوبارہ نارمل موڈ میں آجاتے ہیں۔ اس لئے بینچ مارکنگ نارمل موڈ میں ہی کی جاتی ہے۔

آئی فون 8 سے متعلق اُڑتی افواہوں کی خبر



ایپل کے اگلے آئی فون کے لئے افواہیں اور قیاس آرائیاں شدت پکڑ گئی ہیں۔ ہر بار کی طرح آئی فون میں جادوئی فیچرز شامل کئے جانے کی افواہیں سرگرم ہیں۔ان میں سے کچھ افواہیں حد سے زیادہ مبالغہ آمیز جبکہ کچھ افواہیں حقیقت سے قریب تر ہیں۔ایپل کے مصنوعات کے متعلق قیاس آرائی کرنے والی بیشتر ویب سائٹس اس بات پر متفق نظر آتی ہیں کہ آئی فون کے اگلے ورژن میں بڑے سائز کی اسکرین نصب ہوگی۔جبکہ وائرلیس چارجنگ کی ایڈوانس ٹیکنالوجی کے استعمال کے بارے میں بھی یہ ذرائع خاصی باتیں کررہے ہیں۔دعویٰ کیا جارہا ہے کہ ایپل آئی فون کے اگلے ورژن میں جو وائرلیس ٹیکنالوجی استعمال کی جائے گی،اس کی بدولت اس فون کو چارجنگ پیڈ پر رکھنے کی ضرورت نہیں رہے گی۔

اسی دوران ایک رپورٹ آئی ہے جس میں دعوی کیا گیا ہے کہ ایپل نے وائرلیس چارجنگ کے لئے درکار ضروری پارٹس کے لئے چین کی ایک کمپنی سے معاہدہ کیا ہے اور ایپل اس بار آئی فون میں وہ وائرلیس چارجنگ ٹیکنالوجی استعمال کرنے جارہا ہے جس اس سے پہلے کسی اسمارٹ فون میں استعمال نہیں کی گئی۔

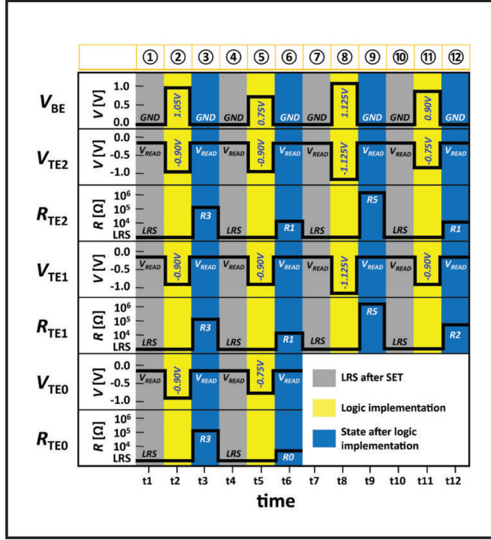
DigiTimes نے چین کے ایک میڈیا ہاؤس کا حوالہ دیتے ہوئے لکھا ہے کہ تائیوان کی سیمی کنڈکٹر کمپنی Lite-on نے ایپل کو GPP بِرج ریکٹی فائر فراہم کرنے کا معاہدہ کیا ہے جنہیں iPhone 8 میں وائرلیس چارج کے لئے استعمال کیا جائے گا۔Lite-on اور ایپل کا تعلق ایک دہائی سے بھی زیادہ پرانا ہے۔یہ کمپنی ایپل کی مصنوعات کے لئے سیمی کنڈکٹر آلات فراہم کرتی ہے۔رپورٹ میں یہ بھی کہا گیا ہے کہ لائٹ اون کو آئی فون کے لئے درکار کل ریکٹی فائرز میں سے آدھے فراہم کرنے کا آرڈر دیا گیا ہے۔نصف ممکنہ طور پر کسی دوسری کمپنی سے حاصل کئے جائیں گے۔

ساتھ ہی یہ افواہ بھی چل رہی ہے کہ Energous نامی کمپنی بھی وائرلیس ٹیکنالوجی کے لئے ایپل کے ساتھ مل کر کام کررہی ہے۔اس کمپنی نے گزشتہ سال اپنی WattUp ٹیکنالوجی کا عملی مظاہرہ پیش کیا تھا۔اس ٹیکنالوجی کی بدولت کسی ڈیوائس کو دور سے بھی چارج کیا جاسکتا ہے۔اس وقت دستیاب وائرلیس چارجنگ فونز کو ایک چارجنگ پیڈ کے اوپر رکھنا پڑتا ہے۔اس دوران اگرچہ فون کے ساتھ کوئی چارجنگ کیبل تو نہیں لگی ہوتی لیکن فون تقریباً ناقابل استعمال ہوجاتا ہے۔کیونکہ چارجنگ کے لئے بہرحال اسے پیڈ کے اوپر چھوڑنا پڑتا ہے۔

لانگ رینج وائرلیس چارجنگ کے حوالے سے ایپل نے کچھ ایجادات بھی پیٹنٹ کروائی ہیں جس سے ظاہر ہوتا ہے کہ ماضی میں کمپنی لانگ رینج وائرلیس چارجنگ کے تجربات کرتی رہی ہے۔اس وقت صرف ایپل واچ ہی وہ واحد پراڈکٹ ہے جس میں وائرلیس چارجنگ ٹیکنالوجی استعمال کی گئی ہے۔ایپل آئی فون 8 کے بارے میں دعویٰ کیا جارہا ہے کہ اس میں دور سے ہی چارج ہوجانے کی صلاحیت ہوگی۔یعنی فون آپ کے ہاتھ میں ہوگا،آپ اسے استعمال کررہے ہونگے،ساتھ ہی وہ چارج بھی ہورہا ہوگا۔

حال ہی میں آئی فون کی دسویں سالگرہ کے موقع پر ایپل کے سی ای او ٹم کُک کا کہنا تھا کہ ایپل کے جانب سے سب سے بہتر پراڈکٹ آنا ابھی باقی ہے۔

انوکھی میموری، جو پروسیسر بھی ہے



سنگا پور اور جرمنی کے کمپیوٹر سائنسدانوں نے ایسی انوکھی ریم چپ تیار کی ہے جو صرف ڈیٹا ہی محفوظ نہیں کرتی بلکہ کمپیوٹر پروسیسر کے طور پر بھی کام کرتی ہے۔

سائنسدانوں نے اس ریم کو بنانے کے لیے جدید ترین میموری چپس جنہیں ری-ریم (Resistive Switching Random Access Memory) کہا جاتا ہے، استعمال کیا ہیں۔ اس نئی ریم کی بدولت تیز رفتار اور مزید پتلے موبائل ڈیوائسز بنانا ممکن ہو سکے گا۔

آج کے کمپیوٹروں میں پروسیسنگ کے لئے ڈیٹا کو میموری سے پروسیسر میں منتقل کرنا پڑتا ہے۔ اس سے صرف وقت ہی ضائع نہیں ہوتا، بلکہ توانائی بھی خرچ ہوتی ہے۔

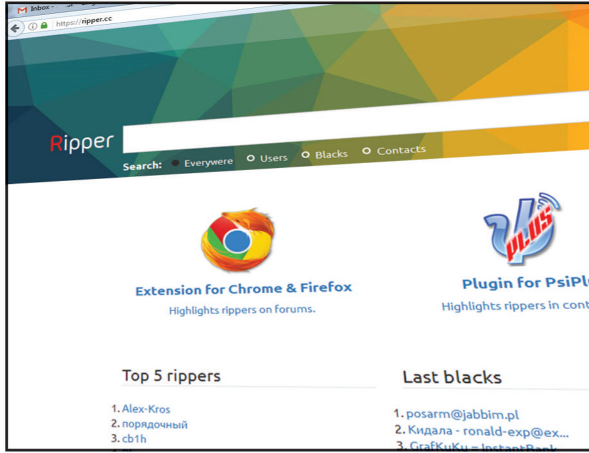
سنگا پور کی نانیانگ ٹیکنالوجیکل یونیورسٹی (این ٹی یو) کے اسسٹنٹ پروفیسر انوپم چٹوپدھایا (Chattopadhyay) کا کہنا ہے کہ یہ کسی شخص سے ایک چھوٹے مترجم کی مدد سے لمبی گفتگو کرنے کی طرح ہے، جس میں وقت بھی ضائع ہوتا ہے اور مشقت بھی کافی اٹھانی پڑتی ہے۔ انوپم کا کہنا ہے کہ اب ہم مترجم کی گنجائش بڑھانے کی صلاحیت رکھتے ہیں، جس سے یہ ڈیٹا کو زیادہ تیزی سے پروسس کر سکتا ہے۔

محققین کا ماننا ہے کہ نیا سرکٹ چونکہ اسٹوریج اور پروسیسر کے درمیان ڈیٹا ٹرانسفر کے وقت کو ختم کر دیتا ہے اس لیے یہ لیپ ٹاپ اور موبائل کے پروسیسر کی رفتار بھی دوگنا بڑھا سکتا ہے۔ میموری چپ کو کمپیوٹیشن کے قابل بنانے سے پروسیسر کی ضرورت نہیں رہے گی۔ یعنی ڈیوائس میں جگہ بچ جائے گی۔ جس سے پتلے، چھوٹے اور ہلکے برقی آلات بنائے جا سکیں گے۔ اسے ویئر ایبل ڈیوائسز اور گھریلو مصنوعات کو جدید بنانے کے لئے بھی استعمال کیا جا سکتا ہے۔

میم رِسٹر (memristor) کے نام سے بھی جانی جانے والی ReRAM کو سین ڈسک اور پیناسونک بنایا ہے اور یہ اس وقت تجارتی طور پر دستیاب دنیا کی تیز ترین میموری چپس ہیں۔ انہیں پہلے ہی انٹرنیٹ آف تھنگ ڈیوائسز میں استعمال کیا جا رہا ہے۔ 2015ء ایچ پی اور اور سین ڈسک نے ReRAM پر مبنی اسٹوریج کلاس میموری (SCM) بنانے کے لیے مشترکہ معاہدہ کیا تھا جس کے بارے میں کہا جا رہا ہے کہ DRAM کا متبادل ثابت ہو گی اور NAND میموری سے ایک ہزار گنا تک تیز رفتار ہو گی۔ ری ریم کو کئی سالوں سے اسٹوریج ٹیکنالوجی بنانے کی کوشش کی جا رہی تھی لیکن این ٹی یو اور آر ڈبلیو ٹی ایچ یونیورسٹیوں کے ماہرین نے پہلی بار اس بات کا مظاہرہ کیا ہے کہ اس سے ڈیٹا کو بھی پروسس کیا جا سکتا ہے۔

آج کے کمپیوٹر پروسیسر بائنری سسٹم کا استعمال کرتے ہیں جہاں ڈیٹا کی بٹس کو 0 یا 1 سے ظاہر کیا جاتا ہے۔ مثال کے طور پر حرف A کو 01000001 کے طور پروسس اور محفوظ کیا جاتا ہے، جو 8 بٹ کیریکٹر ہے۔ لیکن انوپم اور معاونین کے بنائے ReRAM سرکٹ میں ڈیٹا کو دو اعداد میں نہیں بلکہ تین اعداد یعنی 0، 1 اور 2 کے طور پر پروسس اور محفوظ کیا جا سکتا ہے۔ یہی وہ انوکھا پن ہے جس کی بدولت یہ میموری بائنری سسٹم پر چلنے والی میموری کے مقابلے میں زیادہ ڈیٹا محفوظ کر سکتی ہے۔ اس سسٹم کو ٹرنری سسٹم کہا جاتا ہے۔ محققین کا کہنا ہے کہ چونکہ ری-ریم ایک الگ قسم کی برقی مزاحمت کا استعمال کرتی ہے، اس لئے 3 کے بجائے زیادہ حالتوں میں بھی ڈیٹا محفوظ کر سکتی ہے جس سے اس کی گنجائش اور طاقت میں مزید اضافہ ہو جائے گا۔

بے ایمانی کے کام میں مزید بے ایمانی نہیں برداشت



جرم کرنا کسی کے لئے بھی آسان کام نہیں۔ خاص طور سائبر جرائم کرنا آسان کام ہے نہ بچوں کا کھیل۔ لیکن یہ مشکل اُس وقت اور بڑھ جاتی ہے جب مجرم کے پیچھے صرف قانون نافذ کرنے والے ادارے اور پرائیوٹ سکیوریٹی کمپنیاں ہی نہ ہوں بلکہ دوسرے چھوڑے موٹے سائبر کرمنل بھی ہوں جو موقع ملتے ہی چونا لگانے کے تیار بیٹھے ہوں۔ یعنی چوروں کو اپنی ہی صفوں میں موجود چوروں سے خطرہ پیدا ہو گیا ہے۔ دلچسپ بات یہ ہے کہ سائبر مجرموں کی اس پریشانی یا خطرے کو دور کرنے کے لئے ویب سائٹ بھی متعارف کی جا چکی ہے۔

Ripper.cc پر پچھلے سال جون سے مشہور سائبر مجرموں اور دھوکے بازوں کا ڈیٹا بیس بنایا جا رہا ہے۔ سائبر سکیورٹی فرم ڈیجیٹل شیڈوز (Digital Shadows)، جو سارے معاملے کی تحقیق کر رہی ہے، کا کہنا ہے کہ اس ڈیٹا بیس سے آن لائن بلیک مارکیٹ پروان چڑے گی۔

ڈیجیٹل شیڈوز کا کہنا ہے کہ سائبر مجرموں کی دنیا میں دھوکہ دہی بھی ایک قابل نفرت کام ہے۔ فلمی ڈائیلاگ کی شکل میں کہیں تو بے ایمانی کا کام بھی ایمانداری سے کیا جاتا ہے۔ کچھ ہیکر ان مجرموں کے جھنڈ میں چوری میں بھی ایمانداری کو اپنی عزت سمجھتے ہیں جبکہ کچھ ہیکر ایسے بھی ہیں جو جعلی چیزیں مثلاً نا قابل استعمال کریڈٹ کارڈ نمبر اور صارفین کا جعلی ڈیٹا فروخت کر کے پیسے کماتے ہیں۔ چونکہ ان چیزوں کے خریدار بھی مجرم ہی ہوتے ہیں، اس لئے سائبر مجرموں کو بھی جعلی اشیاء سے تحفظ کی ضرورت محسوس ہونے لگی ہے۔ اب ظاہری بات ہے کہ وہ اس کے لئے کسی قانون نافذ کرنے والے ادارے کی مدد نہیں لے سکتے۔ اس کا نتیجہ یہ نکلا کہ سائبر حملے زیادہ پرکشش نہیں رہے، اس ماحول میں کام کرنا مزید خطرناک ہو گیا اور بلیک مارکیٹ میں مندی ہے۔

تاہم Ripper.cc مشہور فراڈیوں کا ایک ڈیٹا بیس بنا رہی ہے، جس میں اب تک 1000 کے قریب پروفائل جمع ہو چکے ہیں۔ ہر پروفائل میں فراڈیے کا اسکرین نیم، اس کے رابطہ کرنے کے طریقوں اور فراڈ کی تفصیلات درج ہے۔ سائٹ پر وزٹ کرنے والے صارفین ایسے کسی نئے فراڈیئے کے لیے نیا پروفائل بھی بنا سکتے ہیں جنھوں نے انہیں لوٹا ہو۔ اس کے ساتھ ویب سائٹ ایک تھرڈ پارٹی سافٹ ویئر ایکسٹینشن بھی فراہم کرتی ہے۔ یہ ایکسٹینشن کروم، فائر فاکس اور انسٹنٹ میسیجنگ اپلی کیشن Jabber میں فراڈیوں کے نام سامنے آنے پر ہائی لائٹ بھی کر سکتی ہے۔ تاکہ اگر کوئی ہیکر ممکنہ فراڈیئے سے کوئی معاملہ طے کرنے جا رہا ہے تو پہلے ہی چوکنا ہو جائے۔

اگرچہ Ripper.cc کا انٹرفیس انگریزی کا ہے مگر اس سائٹ کا منصوبہ 2015 کے وسط میں ایک روسی انڈر گراؤنڈ فورم Exploit.in پر پیش کیا گیا۔ اسی وجہ سے سائٹ پر بہت سے پروفائل روسی زبان میں لکھے ہوئے ہیں۔ اس وقت ویب سائٹ روسی اشتہاروں سے پیسے کما رہی ہے۔ اس کے علاوہ یہ موبائل ایپ اور ہیکروں کے لیے محفوظ طریقے سے غیر قانونی چیزیں خریدنے اور فروخت کرنے کی خدمات سے بھی پیسے بنانے پر غور کر رہی ہے۔

سکیورٹی فرم کا کہنا ہے کہ یہ سائٹ ہیکنگ کے انڈسٹریلائزیشن اور سائبر جرائم میں بڑھتی ہوئی پیشہ وری کی مثال ہے۔

آپ کی تصویر سے بائیومیٹرک ڈیٹا چوری ہوسکتا ہے



بہت سے لوگو پہلے سے جانتے ہیں کہ انہیں سوشل میڈیا پر اپنی حساس اور نجی معلومات فراہم کرنے والی تفصیلات پوسٹ نہیں کرنی چاہیے۔ ایسی چیزوں میں پتے کے ساتھ خطوط یا جہاز کے ٹکٹ یا ملازمت ملنے کا لیٹر وغیرہ خاص طور پر نمایاں ہیں۔ دھوکے باز ان تفصیلات کو بہت آسانی کے ساتھ آپ کے خلاف استعمال کر سکتے ہیں۔ اور اپنا پاس ورڈ تو کسی بھی صورت کسی کو نہیں بتانا چاہئے۔ چاہے آپ کا پاس ورڈ کتنا ہی پرانا ہو چکا ہو اور آپ اسے استعمال کرنا بھی بند کر چکے ہوں۔ اکثر آپ کا پرانا پاس ورڈ آپ کے نئے ممکنہ پاس ورڈ کی پیش گوئی کر سکتا ہے۔

ہوسکتا ہے کہ آپ اپنی تصاویر جن میں کوئی نجی معلومات نہ ہوں، سوشل میڈیا پر شیئر کرنا محفوظ سمجھتے ہوں۔ اگر ایسا ہی ہے کہ آپ بھی دنیا کے کروڑوں دوسرے لوگوں کی طرح ہی سوچتے ہیں۔ لیکن ایسا نہیں ہے۔ تحقیق سے پتا چلا ہے کہ امن کے نشان، یعنی دو انگلیوں سے وکٹری کے نشان یا پورے ہاتھ والی تصاویر پوسٹ کرنا بھی سیکورٹی کے لیے خطرہ ہے۔ اب ہیکر اس قابل ہو چکے ہیں کہ ایسی کسی تصویر سے آپ کے فنگر پرنٹ حاصل کر سکیں جو کہ آپ کے فون، کمپیوٹر یا ٹیبلٹ کے لیے چابی کی حیثیت رکھتا ہے۔

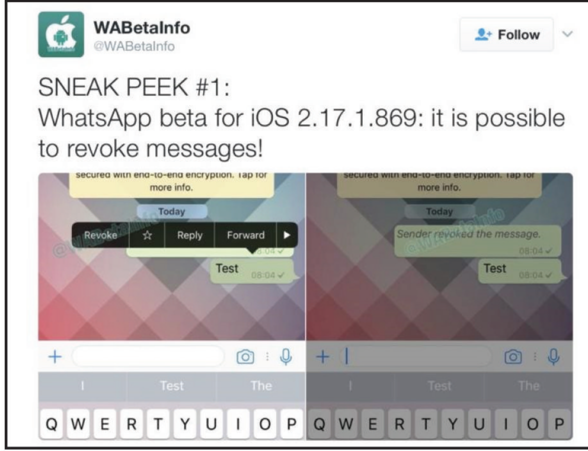
جاپان کے نیشنل انسٹیٹیوٹ آف انفارمیٹکس (این آئی آئی) کے ماہرین کا کہنا ہے کہ تین میٹر کے فاصلے سے لی گئی تصاویر میں سے بغیر کوئی جدید یا نئی ٹیکنالوجی استعمال کیے، فنگر پرنٹ آسانی سے حاصل کیے جاسکتے ہیں۔

یہ پہلی بار نہیں کہ بائیومیٹرک سیکوریٹی نظام پر سوال اٹھے ہوں۔ سال 2015 میں جان "سٹار بگ" کریسلر نام کے ایک ہیکر نے جرمن چانسلر انجیلا مرکل کی آنکھ کی پتلی کے نشانات کامیابی سے ان کی تصویر سے اخذ کرنے کا مظاہرہ کیا تھا۔ آنکھ کی پتلی کے نشانات بھی انگلیوں کے نشانات کی طرح ہر انسان میں منفرد ہوتے ہیں اور انہیں کسی شخص کو شناخت کرنے کے لئے کئی برسوں سے استعمال کیا جارہا ہے۔

اگر آپ کے ای میل اکاؤنٹ یا موبائل فون کا پاس ورڈ کسی کو معلوم ہوجائے تو آپ پاس ورڈ تبدیل کر کے اپنے ای میل اکاؤنٹ یا موبائل فون کو دوبارہ محفوظ بنا سکتے ہیں۔ لیکن بائیومیٹرکس یعنی انگلیوں یا آنکھ کی پتلی کے نشانات کو تبدیل کرنا ممکن نہیں۔ اس لئے بائیومیٹرک انفارمیشن کے عام ہوجانے سے آپ کی سیکوریٹی ہمیشہ خطرے میں رہتی ہے۔ ایک بائیومیٹرک کمپنی NuData Security میں کام کرنے والے روبرٹ کیپس کا کہنا ہے کہ ہم جہاں کہیں بھی جاتے ہیں، وہاں پر اپنا بائیومیٹرک ڈیٹا چھوڑ دیتے ہیں۔ جس چیز کو ہم چھوتے ہیں، اس پر ہمارے فنگر پرنٹ ہوتے ہیں۔ سوشل میڈیا پر سیلفی پوسٹ کرنا، دوستوں اور گھر والوں کے ساتھ ویڈیو شیئر کرنا یہ سب آپ کی بائیومیٹرک معلومات حاصل کرنے کا ذریعہ بن سکتا ہے۔ ایک بار بائیومیٹرک ڈیٹا چرا کر ڈارک ویب پر فروخت کر دیا جائے تو اس صارف کی موت تک اس کے اکاؤنٹ تک رسائی کی کوشش کی جاسکتی ہے۔

این آئی آئی کی ٹیم نے صرف مسئلہ ہی نہیں، اس کا حل بھی تلاش کیا ہے۔ انہوں نے ٹائٹینیم آکسائیڈ کی مدد سے ایک شفاف فلم تیار کی ہے جسے اگر انگلیوں کے پوروں پر لگا یا جائے تو ہیکر تصویر سے فنگر پرنٹ نہیں حاصل کر سکیں گے۔ تاہم اس حفاظتی ٹیکنالوجی کو مکمل طور پر تیار ہونے میں 2 سال کا عرصہ لگ سکتا ہے۔

وٹس ایپ کا نیا فیچر، آ بھی سکتا ہے اور نہیں بھی



اکثر ایسا ہوتا ہے کہ آپ میسج مکمل ٹائپ کرنے سے پہلے ہی Send کا بٹن دبا کر بھیج دیتے ہیں، جس سے ادھورا یا ذو معنی جملہ منزل تک پہنچ کر آپ کے لئے شرمندگی کا باعث بنتا ہے۔ ایسا بھی ہوتا ہے کہ لوگ غلطی سے اپنے ساتھی کو بھیجا جانے والا پیغام اپنے باس کو بھیج دیتے ہیں یا پیغام لکھتے ہوئے املاء کی سنگین غلطی کر دیتے ہیں، جس کا احساس پیغام بھیجنے کے بعد ہوتا ہے۔ دوسری میسجنگ ایپس کی طرح وٹس ایپ پر بھی اب تک ایسا ہی تھا کہ بھیجا ہوا پیغام ایسے ہی تھا جیسے منہ سے نکلی بات یا کمان سے نکلا تیر، جو واپس نہیں آ سکتا۔

حال ہی میں WABetaInfo نے ٹوئٹر پر وٹس ایپ کے بی ٹا ورژن کا ایک اسکرین شاٹ شیئر کیا تھا جس میں دیکھا جا سکتا ہے کہ وٹس ایپ کے ذریعے بھیجے گئے پیغامات کو ڈیلیٹ کیا جا سکتا ہے یا ان کی تدوین کی جا سکتی ہے۔ اس فیچر کے تحت جس شخص کو بھیجا گیا میسج ڈیلیٹ کیا جائے گا اسے بعد میں میسج ڈیلیٹ ہونے کا پتا چل جائے گا یعنی میسج کا ڈیلیٹ ہونا ریکارڈ پر آ جائے گا۔ اگر آپ نے مائیکروسافٹ اسکائپ پر کبھی اپنا بھیجا ہوا پیغام ڈیلیٹ یا اس کی تدوین کی ہے تو آپ با آسانی سمجھ سکتے ہیں کہ وٹس ایپ کا مذکورہ فیچر کس طرح کام کرے گا۔

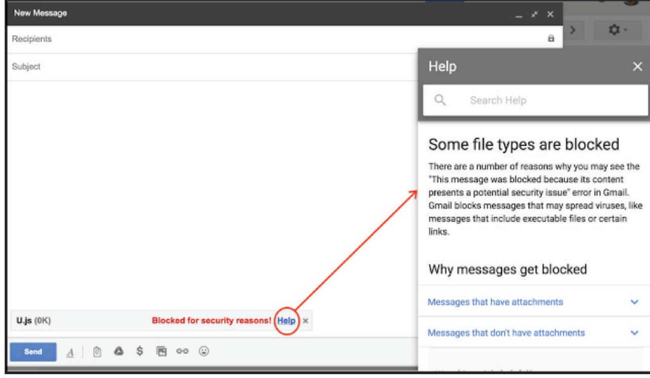
اگر وٹس ایپ پر بھیجا گیا پیغام وصول کنندہ پڑھ چکا ہے تو اس پیغام کو ڈیلیٹ کرنا یا ایڈٹ کرنا ممکن نہیں رہے گا۔ یعنی صارفین اپنے بھیجے گئے پیغام کو فوراً ڈیلیٹ یا ایڈٹ کرنا ہوگا۔ پیغام کے پڑھے جانے کے بعد کچھ نہیں کیا جا سکے گا۔ وٹس ایپ اپنا یہ فیچر اینڈرائیڈ اور آئی او ایس دونوں آپریٹنگ سسٹمز میں جانچ رہا ہے۔ اس کے علاوہ وٹس ایپ دیگر بہت سے فیچر بھی مستقبل قریب میں متعارف کرا سکتا ہے۔ اس میں سب سے اہم گروپ میں دوستوں کے ساتھ براہ راست اپنی لوکیشن شیئر کرنا ہے۔ یعنی آپ کے دوست، آپ کی مرضی سے، جان سکیں گے کہ آپ اس وقت کہاں موجود ہیں۔

اگرچہ گوگل پلے اسٹور سے وٹس ایپ کا بی ٹا ورژن ڈاؤن لوڈ کیا جا سکتا ہے۔ لیکن فی الحال وہاں دستیاب بی ٹا ورژن میں بھیجے گئے پیغام کو ڈیلیٹ کرنے یا تدوین کرنے کا فیچر موجود نہیں۔ بی ٹا ورژن میں شامل کسی فیچر کے بارے میں حتمی طور پر نہیں کہا جا سکتا کہ وہ کب فائنل ورژن میں جاری کیا جائے گا یا جاری کیا بھی جائے گا یا نہیں۔ اس سارے عمل میں چند ہفتے یا چند ماہ بھی لگ سکتے ہیں۔ وٹس ایپ ماضی میں کئی فیچرز جانچ کر انہیں ترک کر چکا ہے۔ اس لئے اگر وٹس ایپ کو اس فیچر کے حوالے سے اچھی فیڈ بیک نہ ملی تو عین ممکن ہے کہ یہ فیچر آپ کبھی بھی وٹس ایپ میں نہ دیکھ سکیں۔ البتہ ہم یہ سمجھتے ہیں کہ پیغام کو ڈیلیٹ کرنے یا اس کی تدوین کرنے کا یہ فیچر وقت کی ضرورت ہے اور وٹس ایپ کو اسے فائنل ایپلی کیشن میں ضرور شامل کرنا چاہئے۔

	WhatsApp Indicator	Meaning
1.	(clock)	Message hasn't left your phone yet
2.	(single grey tick)	Message sent to WhatsApp Server
3.	(double grey tick)	Message delivered to recipient's phone
4.	(double blue tick)	Recipient has read the message
5.	(green mic)	Voice delivered to recipient's phone
6.	(blue mic)	Voice has been heard by recipient

TechGainer.com

جی میل کیلئے جاوا اسکرپٹ فائلیں ناقابل قبول



تیرہ فروری کے بعد جی میل کسی ای میل کے ساتھ جاوا اسکرپٹ فائل منسلک (اٹیچ) کرنے کی اجازت نہیں دے گا۔ اس طرح گزشتہ کئی سالوں سے مال ویئر پھیلانے کی ایک اہم وجہ کا خاتمہ ہوجائے گا۔

اس وقت جی میل آپ کو کوئی بھی ایسی فائل ای میل کے ساتھ منسلک نہیں کرنے دیتا جو کہ ایگزی کیوٹ ہوسکتی ہو یا اس میں وائرس ہو۔ حتیٰ کہ اگر کسی وائرس کو زِپ فائل کی شکل میں منسلک کرنے کی کوشش کی جائے تو بھی جی میل اس کوشش کو ناکام بنا دیتا ہے۔ اب نئی تبدیلی کے بعد اگر کوئی شخص JS. فائل کسی ای میل کے ساتھ براہ راست یا پھر کسی کمپریس فارمیٹ مثلاً زِپ، gzip، bz2، gz وغیرہ میں بھیجنے کی کوشش کرے گا تو ای میل پیغام بھیجنا ہی ممکن نہیں رہے گا۔ یہ ویب ڈیویلپرز اور پروگرامرز کے لئے قدرے پریشانی کا باعث ہوسکتی ہے جو اکثر جاوا اسکرپٹ کی فائلیں بذریعہ ای میل ایک دوسرے کو بھیجتے ہیں۔ تاہم یہ لوگ اب بھی گوگل ڈرائیو پر جاوا اسکرپٹ فائل اپ لوڈ کرکے اس کا لنک بھیج سکتے ہیں۔ دوسری جانب JS. فائل کو اٹیچ کرنے کی اجازت نہ دینے سے مال ویئر کی روک تھام ہوسکے گی۔ ہم قارئین کو بتاتے چلیں کہ اس وقت دو درجن سے زائد فائل ایکسٹینشن ایسے ہیں جنہیں جی میل پر بذریعہ اٹیچمنٹ ارسال نہیں کیا جاسکتا۔ اس فہرست میں درج ذیل ایکسٹینشن شامل ہیں:

.ADE, .ADP, .BAT, .CHM, .CMD, .COM, .CPL, .EXE, .HTA, .INS, .ISP, .JAR, .JSE, .LIB, .LNK, .MDE, .MSC, .MSP, .MST, .PIF, .SCR, .SCT, .SHB, .SYS, .VB, .VBE, .VBS, .VXD, .WSC, .WSF and .WSH.

یہ ساری ایسی فائلیں جنہیں ماضی میں وائرس پھیلانے کے لئے استعمال کیا جاتا رہا ہے۔ اب ایسا ہی معاملہ JS فائلوں کے ساتھ ہے جو مائیکروسافٹ ونڈوز میں ونڈوز اسکرپٹ ہوسٹ کی بدولت براہ راست ایگزی کیوٹ ہوسکتی ہیں۔ وائرس بنانے والے اس بات کا فائدہ اٹھا کر معصوم لوگوں کو ایسے جاوا اسکرپٹ بھیجتے ہیں جو ایگزی کیوٹ ہونے پر سسٹم میں مال ویئر ڈاؤن لوڈ اور انسٹال کر دیتے ہیں۔ معروف رانسم ویئر Locky کو پھیلانے کے لئے اس تکنیک کا بھی استعمال کیا جاتا رہا ہے۔ ایک دوسرا رانسم ویئر جسے RAA کے نام سے جانا جاتا ہے، وہ تو مکمل طور پر جاوا اسکرپٹ میں ہی بنایا گیا ہے۔

ای میل کے ذریعے وائرس پھیلانے کی کہانی اتنی ہی پرانی ہے جتنی خود وائرس کی تاریخ ہے۔ بیشتر ویب ای میل سروسز جیسے جی میل، لائیو وغیرہ صارفین کو موصول ہونے والے ای میل پیغامات کو اسکین کر کے پہلے ہی خبردار کر دیتے ہیں کہ اس میں وائرس ہے۔ لیکن وہ افراد جو ان سروسز کے بجائے اپنی ای میل سروس استعمال کرتے ہیں، انہیں ان وائرسز سے خطرہ ہمیشہ رہتا ہے۔ اس لئے ماہرین مشورہ دیتے ہیں کہ ای میل کے ساتھ منسلک کسی بھی ایسی فائل کو ڈاؤن لوڈ نہ کریں جو ایگزی کیوٹ ایبل ایکسٹینشن میں ہو یا اسے کسی ایسے شخص نے بھیجا ہو جسے آپ جانتے ہی نہیں۔ اگر آپ کو بذریعہ ای میل مائیکروسافٹ ورڈ کی کوئی فائل موصول ہوئی ہے تو بغیر اینٹی وائرس سے اسکین کئے اسے بھی کھولنا خطرناک ہے۔

ڈونلڈ ٹرمپ کا حکم، اسٹارٹ اپ کمپنیاں مخمصے کا شکار



امریکہ اس وقت زبردست تبدیلیوں کی زد میں ہے۔ صدر ڈونلڈ ٹرمپ نے اپنے انتخابی ایجنڈے پر عمل کرتے ہوئے 7 ممالک کے باشندوں کا امریکہ میں داخلہ بند کردیا ہے۔ اپنے صدارتی حکم نامے میں دراصل انہوں نے شامی مہاجرین کو امریکا میں داخلے سے روکنے کے لیے امریکی مہاجرین کے پروگرام کو 120 دن کے لیے بند کردیا تھا۔ اس کے علاوہ انہوں نے 7 مسلمان ممالک، ایران، عراق، لیبیا، صومالیہ، سوڈان، شام اور یمن کے شہریوں کو 90 دن کے لیے امریکا میں داخل ہونے سے روک دیا۔ اس حکم کے آتے ہی امریکا میں ایک نیا احتجاجی سلسلہ شروع ہوگیا جو دوسرے ممالک تک پھیل گیا۔ اگرچہ یہ حکم فی الحال امریکی عدالت نے معطل کررکھا ہے، لیکن امریکی صدر کو حاصل خصوصی اختیارات دیکھتے ہوئے یہ بھی ممکن ہے کہ اعلیٰ عدلیہ ماتحت عدلیہ کے فیصلے کو ختم کردیں اور یہ پابندی بحال ہوجائے۔

اس پابندی کا براہ راست امریکی ٹیکنالوجی کمپنیوں پر پڑا ہے۔ مائیکروسافٹ، فیس بک، الفابیٹ، گوگل، یاہو!، ایپل سمیت درجنوں بڑی کمپنیاں اس پابندی کے خلاف ہیں اور انہوں نے اس صدارتی حکم نامے کو عدالت میں چیلنج کررکھا ہے۔ ان کمپنیوں کو کئی خدشات ہیں۔ بات اگر صرف 7 مسلمان ممالک تک محدود رہنے کی گارنٹی ہوتی تو شاید یہ کمپنیاں برداشت کرجاتیں، لیکن صدر ڈونلڈ ٹرمپ سے ہرگز بعید نہیں کہ وہ دیگر مسلمان ممالک کے خلاف بھی ایسی ہی پابندی عائد کردیں۔ امریکی ٹیکنالوجی کمپنیوں میں ایک بڑی تعداد مسلمانوں کی کام کرتی ہے اور کئی کمپنیاں جو آج امریکہ کی پہچان ہیں وہ دراصل مہاجرین کی قائم کردہ ہیں۔ امریکہ کی کم و بیش ہر بڑی کمپنیوں میں مہاجرین کسی نہ کسی حیثیت سے کام کررہے ہیں، خاص طور پر انفارمیشن ٹیکنالوجی کی صنعت سے وابستہ کمپنیوں میں یہ تناسب بہت زیادہ ہے۔

اس نئے آرڈر نے جہاں پہلے سے قائم اور مستحکم کمپنیوں میں پریشانی پیدا کی ہے، وہیں اسٹارٹ اپ کمپنیوں میں کھلبلی مچا رکھی ہے۔ سیلکان ویلی میں وینچرل کیپٹلسٹ کیٹ مچل نے تمام اسٹارٹ کمپنیوں سے کہا ہے کہ وہ اپنے ملازمین کو فی الحال امریکہ سے باہر نہ جانے کا مشورہ دیں۔ سیلکان ویلی میں کام کرنے والے افراد کی اکثریت دنیا کے دیگر ممالک سے تعلق رکھتی ہے۔ نئے کاروبار ساری دنیا سے ہنرمند لوگوں کو ملازمت پر رکھ رہے ہیں۔ ان کاروباری اداروں کی ضرورت ہے کہ ساری دنیا میں گاہک تلاش کریں اور سلیکون ویلی میں وینچر کیپٹلسٹ کمپنیوں کی مدد سے سرمایہ حاصل کریں۔

سیلکان ویلی کی سب سے پرانی کمپنیوں میں سے ایک Bessemer Venture Partners کا کہنا ہے کہ ان دنوں کاروباری ادارے اس وجہ سے اپنا کاروبار روک رہے ہیں کہ ان کے ملازمین امریکہ سے جانے کے بعد دوبارہ واپس امریکہ نہیں آسکتے۔ 2017ء میں کاروباری نقصانات کی سب سے بڑی وجہ یہی ہوگی۔ امریکا میں امیگریشن کا بحران تیزی سے بڑھ رہا ہے۔ اس بحران کی وجہ سے امریکی کمپنیاں ٹیکنالوجی کی عالمی کمپنیوں کے مقابلے میں کم کاروبار کرپائیں گی۔ اس بحران سے بے روزگاری بھی بڑھے اور امریکی سرمایہ دار اپنا سرمایہ ملک سے باہر بھی منتقل کریں گے۔ اس بحران کا اسٹارٹ اپ پر کتنا اثر ہوا ہے یا ہوگا، اس کا اندازہ لگانا ابھی مشکل ہے۔ لیکن 15 سے زائد وینچر کیپٹلسٹ اور ٹیکنالوجی کمپنیوں کے بانیوں نے سفری پابندی کے فوری اور نقصان دہ اثرات کا خدشہ ظاہر کیا ہے۔

ڈرونز کے ذریعے انٹرنیٹ، الفابیٹ کا منصوبہ ترک



سلیکان ویلی کی ٹیکنالوجی کمپنیوں نے سوچا تھا کہ دور دراز کے علاقوں میں انٹرنیٹ پہنچانا کوئی بڑا مسئلہ ہی نہیں۔ ڈرونز، غباروں اور مصنوعی سیاروں سے دور دراز کے علاقوں میں وہ آسانی سے انٹرنیٹ پہنچا سکتے ہیں۔لیکن اس میدان میں اترتے ہی ان کمپنیوں کو پتا لگا کہ جتنا آسان وہ سوچ رہے تھے، یہ چیز اتنی سادہ بھی نہیں۔ اب اطلاعات ہیں کہ ڈرونز اس معاملے میں خاص طور پر ناکام ثابت ہورہے ہیں۔ الفابیٹ (گوگل کی مالک کمپنی) نے اعلان کیا ہے کہ وہ اپنا ٹائٹن ڈرون کا پروجیکٹ بند کررہی ہے۔اس پروجیکٹ کو دور دراز کے مقامات پر آسمان سے ڈیٹا کنکشن فراہم کرنے کے لیے تجرباتی بنیادوں پر شروع کیا گیا تھا۔حقیقت یہ ہے کہ کمپنی کی ایکس لیب نے ٹائٹن پروجیکٹ کے ڈرون پر 2016 کے شروع میں ہی کام بند کردیا تھا۔کمپنی نے اب بس اسے بند کرنے کا باقاعدہ اعلان کیا ہے۔

کمپنی اب ٹائٹن پروجیکٹ کے بجائے لون (Loon) پروجیکٹ پر اپنی توجہ مرتکز کیے ہوئے ہے جس میں انٹرنیٹ کی فراہمی کے لیے ڈرونز کے بجائے بڑے بڑے ہوائی غباروں کا استعمال کیا جاتا ہے۔الفابیٹ کے ترجمان کا کہنا ہے کہ معاشی اور تکنیکی طور پر پروجیکٹ لون کے ذریعے دنیا کو مربوط کرنا زیادہ قابل عمل ہے۔

فیس بک نے دور دراز کے علاقوں میں انٹرنیٹ کی فراہمی کے لیے ڈرون کا سہارا لیا۔فیس بک نے پچھلے گرما میں ایکوئیلا نام کے ڈرون کا تجربہ کیا لیکن لینڈنگ کے دوران اسے کافی نقصان پہنچا۔نیشنل ٹرانسپورٹیشن سیفٹی بورڈ کا کہنا ہے کہ تیز ہواؤں کے باعث ڈرون کا آٹو پائلٹ سسٹم خراب ہوگیا جس کی وجہ سے اس کی رفتار تیز ہوئی اور یہ زمین سے ٹکرا گیا۔ اس حادثے سے ڈرون کے ذریعے انٹرنیٹ ڈیٹا فراہم کرنے کی ٹیکنالوجی پر بھی سوالات کھڑے ہوگئے۔ ان ڈرونز کو انتہائی بلندی پر کرہ قائمہ (فضا کی ایک تہہ جو زمین کی سطح کے اوپر تقریباً 11 کلومیٹر یا 7 میل سے شروع ہوتی ہے) پر پرواز کرتے ہوئے انٹرنیٹ فراہم کرنے کے لیے ڈیزائن کیا گیا ہے۔ یہ ڈرون زمین کی گردش کے ساتھ ساتھ گردش کرتے، جس کی وجہ سے وہ مسلسل اپنے علاقے میں انٹرنیٹ فراہم کرسکتے ہیں۔ ان ڈرون کو کئی دنوں، ہفتوں یا اس سے بھی زیادہ عرصے فضا میں رہنا پڑتا، اس لیے انہیں شمسی توانائی اور بیٹریوں پر انحصار کرنا پڑتا۔ اس کا مطلب ہے کہ ایسے ڈرون کو وزن میں ہلکا ہونا بھی ضروری ہے۔فیس بک کے ایکوئیلا ڈرون کے پروں کا پھیلاؤ بوئنگ 737 کے پروں کے پھیلاؤ سے بھی زیادہ تھا لیکن کاربن فائبر فریم کی بدولت اس کا وزن 1 ہزار پاؤنڈ سے بھی کم تھا۔

ابھی تک الفابیٹ اور فیس بک دونوں کے پاس انٹرنیٹ فراہم کرنے کے دوسرے منصوبے بھی ہیں۔ الفابیٹ لون پروجیکٹ پر توجہ مرتکز کیے ہوئے ہے جبکہ فیس بک اب مصنوعی سیاروں کی مدد سے انٹرنیٹ فراہم کرنا چاہتا ہے۔فیس بک کی کنکٹیویٹی لیب کے سربراہ یائل ماگوئر نے پچھلے سال کہا تھا کہ ڈرون کے برعکس سیٹلائٹ کے حوالے سے ان کی ترجیحات زیادہ نہیں ہیں۔لیکن ڈرون کے حادثے کے بعد ان کی ترجیحات میں تبدیلی واقع ہوئی ہے۔ میڈیا میں ایسی رپورٹس بھی آئی تھیں کہ مارک زکر برگ ڈرونز کے ذریعے انٹرنیٹ فراہمی کے منصوبے سے زیادہ خوش نہیں۔ ان دونوں اہم کمپنیوں کے ہاتھ کھڑے کرلینے کے بعد اب ڈرونز کے ذریعے وسیع پیمانے پر انٹرنیٹ کی فراہمی کا منصوبہ ممکن نظر نہیں آرہا۔

علمدار حسین

یوٹیوب

چند ٹکوں کے لئے گند سے بھر دیا گیا

آن لائن وڈیوز دیکھنے کے لیے یوٹیوب اس وقت سب سے بڑا پلیٹ فارم ہے۔ گوگل نے 2006 میں یوٹیوب کو خریدنے کے بعد اس میں بے شمار فیچرز متعارف کرائے اور اسے دنیا کی ٹاپ ویب سائٹس کی فہرست میں لا کھڑا کیا۔ اس ویب سائٹ کی مقبولیت اور اہمیت کا اندازہ اس بات سے لگایا جا سکتا ہے کہ اب کئی بڑے میڈیا ہاؤسز اور ٹی وی چینلز بھی اس کا بھرپور فائدہ اُٹھا رہے ہیں۔ ٹی وی چینلز دو طرح سے اس سے فائدہ حاصل کر رہے ہیں۔

پہلا فائدہ تو یہ ہے کہ ان کے پروگرامز جو کہ ایک دفعہ نشر ہونے کے بعد شاید ایک آدھ بار ہی دوبارہ نشر ہوتے ہیں، چینل کے ریکارڈ روم میں دفن ہونے کی بجائے وہ یوٹیوب پر اپ لوڈ کر کے بغیر کوئی پیسہ خرچ کیے ناظرین کے لیے دستیاب ہو جاتے ہیں۔ اس طرح بدستور ان کی مشہوری ہوتی رہتی ہے۔ اور دوسرا بڑا فائدہ یہ ہے کہ یوٹیوب کو اپنی وڈیو میں اشتہارات دِکھانے کی اجازت دے دیں تو اس کے عوض یوٹیوب رقم ادا کرتی ہے۔ اس طرح ٹی وی چینلز کے پروگرامز عوام تک بھی پہنچ جاتے ہیں اور اس کے بدلے وہ مزید رقم بھی کما لیتے ہیں۔ بہر حال یہ تو ایک جائزہ طریقہ ہے جس پر اعتراض نہیں کیا جا سکتا۔

قابلِ اعتراض وہ طریقے ہیں جن میں دوسرے محنت کیے بغیر یوٹیوب سے کمانا شروع ہو جاتے ہیں یا پھر محنت بھی کرتے ہیں تو اتنی غیر معیاری کے وہ دوسروں کے لیے فائدے مند نہیں بلکہ نقصان کا باعث بن سکتی ہے۔

جیسے کہ مارک ٹوئن کا مشہور مقولہ ہے کہ ''صحت پر کتابیں پڑھتے ہوئے محتاط رہیے۔ کتابت کی غلطی سے آپ کی موت بھی واقع ہو سکتی ہے۔''

کمائی بذریعہ غیر اخلاقی مواد

یوٹیوب پر غیر اخلاقی مواد کے ذریعے کمانا تو اب ایک معمولی سی بات بن چکی ہے۔ اس موضوع پر ہم پہلے بھی کئی دفعہ لکھ چکے ہیں لیکن اس پر جتنا بھی لکھا جائے کم ہے۔ انتہائی افسوس سے کہنا پڑتا ہے کہ ہمارے ہاں غیر اخلاقی وڈیوز دیکھنے کا رجحان انتہائی زیادہ ہے اور چونکہ یوٹیوب مقبول وڈیوز کو سب سے پہلے اپنے ہوم پیج پر دکھاتا ہے اس لیے نا چاہتے ہوئے سب کو انھیں بھگتنا پڑتا ہے۔

افسوس کا مقام یہیں ختم نہیں ہوتا، بلکہ یہ دیکھ کر مزید دُکھ ہوتا ہے کہ یہ وڈیوز بنانے والے کوئی غیر ملکی نہیں جو یہ گند ہم پر مسلط کر رہے ہوں بلکہ ہمارے اپنے ہم وطن دوسروں کی دلچسپی کو مدِ نظر رکھتے ہوئے انتہائی غیر اخلاقی موضوعات پر وڈیوز بنا کر اپ لوڈ کر رہے ہیں چونکہ انھیں دیکھنے والوں کی بڑی تعداد موجود ہے اس لیے وہ اپنے چینلز کے ذریعے کمائی کرنے میں بھی مصروف ہیں۔ اگر لوگ ان وڈیوز کو دیکھنا چھوڑ دیں تو ان کو بنانے والوں کی کمائی رُک جائے گی اور نتیجتاً وہ ایسی وڈیوز بنانا بھی بند کر دیں۔

کمپیوٹنگ کے گزشتہ شمارے میں ہم نے ''کلک بیٹ'' پر بھی تفصیلی مضمون شائع کیا ہے جس میں اس بات پر روشنی ڈالی گئی ہے کہ کس طرح یوٹیوب پر ''پُرکشش'' تصویر استعمال کرتے ہوئے لوگ دوسروں کو اپنی وڈیو دیکھنے پر مجبور کر رہے ہیں۔

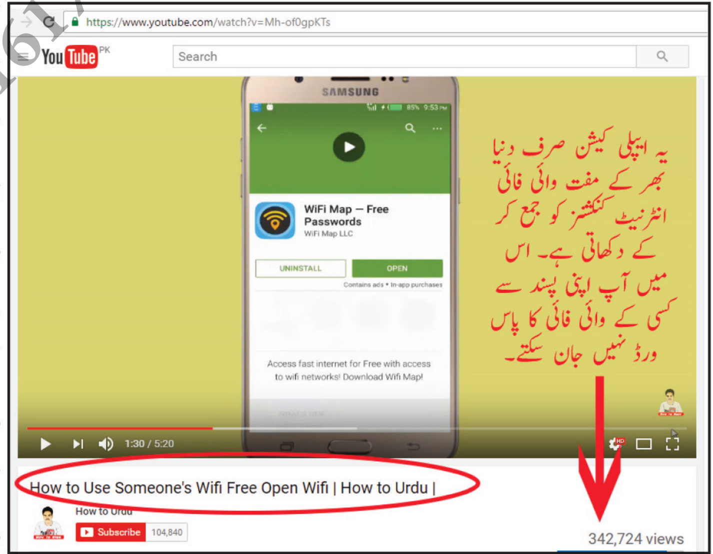
آج کل جو طریقہ رائج ہے اس میں وڈیو بنانے والے یہ نیک حضرات حکیمی



ٹوٹکوں کی سستی سی کتاب سے بس ''ترکیبیں'' اردو میں لکھ کر سلائیڈ شو بناتے ہیں، وڈیو کا عنوان انتہائی ''پُرکشش'' رکھتے ہیں اور ایسی ہی تصویر استعمال کرتے ہیں اور ان کا کام ہو جاتا ہے۔ یہ وڈیو دیکھنے کے لیے لوگ ایسے کھنچے چلے آتے ہیں جیسے سوئی مقناطیس کی جانب۔

اُردو کمپیوٹر چینلز کا انتہائی ابتر معیار

چونکہ ہمارا شعبہ کمپیوٹر ہے تو ہم نے سوچا اس حوالے سے مقبول اُردو چینلز کا جائزہ لیا جائے تو یہاں بھی انتہائی مایوسی کا سامنا کرنا پڑا۔ پیسے کمانے کی خاطر نیم حکیموں نے اس شعبے کو بھی معاف نہیں کیا۔ انتہائی غیر مستند کمپیوٹر ٹپس کو استعمال کرتے ہوئے صاحبان نے وڈیوز بنا کر اپنے چینل پر اپ لوڈ کر رکھی ہیں۔ اصل دُکھ اس وقت ہوتا ہے جب یہ پتا چلتا ہے کہ لاکھوں لوگ اسے دیکھ چکے ہیں اور تبصروں میں داد بھی دے چکے ہیں۔ ایک آدھ جگہ جب ہم نے لوگوں کو اس وڈیو کی حقیقت بتانے کی جرات کی تو اُلٹا ''مریدوں'' نے ہمیں ہی لتاڑ کر بھاگنے پر مجبور کر دیا۔



کیا زیادہ ویوز کامیابی کی علامت ہیں؟

یہاں ایک اور بہت بڑا سوال سامنے آتا ہے کہ کیا کسی وڈیو کے زیادہ سے زیادہ ویوز اس کی کامیابی کا نشان ہیں؟ عموماً تو یہ بات سچ ہی ہے لیکن ہر دفعہ نہیں۔ اگر آپ مقبول پاکستانی میوزک شو ''کوک اسٹوڈیو'' کی مثال دیکھیں تو آپ اس بات کو سمجھ سکتے ہیں۔ اس شو کا آخری سیزن تاریخ کا کامیاب ترین سیزن رہا۔ اس مقبولیت کو اُن کی وڈیوز کو دیکھی گئی تعداد سے ناپا گیا لیکن اس میں ہم نے دو باتوں کو سرے سے نظر انداز کر دیا۔

پہلی بات: آج سے چند سال پہلے ویورز کی تعداد کیا تھی اور آج کیا ہے؟ آج سے چند سال قبل اسمارٹ فونز اور انٹرنیٹ ہر کسی کی دسترس میں نہیں تھا اس لیے وڈیوز کی دیکھی گئی تعداد انتہائی کم ہوتی تھی۔ لیکن آج کل صورتِ حال یکسر مختلف ہے۔ آج بچے بچے کے ہاتھ میں اسمارٹ فون موجود ہے جس پر انٹرنیٹ چل رہا ہوتا ہے۔ اس لیے ہر وڈیو کو دیکھے جانے کی تعداد بڑھ گئی ہے، اب یہ بھی ضروری نہیں کہ کسی نے وڈیو دیکھی تو ضرور اسے پسند کیا ہوگا لیکن یہاں تو صرف دیکھا جانا گِنا جاتا ہے پسندیدگی و ناپسندیدگی کو کہاں توجہ دی جاتی ہے۔ دیکھنے والی عوام بھی ذہن کی انتہائی کچی ہے تو ویوز حاصل کرنا کون سا مشکل کام ہے۔

دوسری بات: فیس بک پر کوئی بھی وڈیو یا پوسٹ جب آپ دیکھیں کہ بلاوجہ آپ کو دِکھائی جا رہی ہے تو اس کی وجہ یہ ہے کہ اپ لوڈ کرنے والے نے اس کام کے فیس بک کو پیسے ادا کر رکھے ہیں۔ یقیناً آپ جانتے ہوں گے کہ کسی پیج کے لاکھوں لائیکس ہونے کے باوجود اُن کی پوسٹ تمام لائیک کرنے

والے لوگوں کو نہیں دکھائی جاتی، لیکن اگر آپ فیس بک کو رقم ادا کرتے ہوئے پوسٹ کو بوسٹ (Boost) کرتے ہیں تو یہ اُن لوگوں کو بھی دِکھائی جائے گی جنھوں نے پیج لائیک نہیں کر رکھا بلکہ اپنی پسند کے اعتبار سے لوگوں تک پوسٹ پہنچائی جاسکتی ہے۔

اچھی بات یہ ہے کہ فیس بک ایسی پوسٹس کے ساتھ Sponsored لکھا دِکھاتی ہے تاکہ صارفین سمجھ سکیں کہ یہ تشہیری پوسٹ ہے۔ اگر آپ غور کرنا شروع کریں تو آپ کو روز ہی اپنی نیوز فیڈ میں ایسی پوسٹس دِکھائی دیں گی۔

دوسروں کی وڈیوز سے کمانا

بھئی یہ طریقہ بہت ہی آسان اور دلچسپ ہے۔ یوٹیوب کی کاپی رائٹس کے حوالے سے پالیسی انتہائی سخت ہے کہ آپ کسی دوسرے کی وڈیو یا میوزک استعمال نہیں کر سکتے لیکن ''ماہرین'' نے اس کا توڑ بھی نکال لیا ہے۔ آج کل یوٹیوب پر بڑی تعداد میں ''ری ایکشنز'' وڈیوز بنائی جا رہی ہے۔ کئی لوگوں کے چینلز صرف اسی کے سہارے چل رہے ہیں۔



اس میں ہوتا یہ ہے کہ یوٹیوب کی ہی کوئی وڈیو دیکھتے ہوئے اپنے تاثرات کو ریکارڈ کیا جاتا ہے۔ مثلاً کوئی مزاحیہ وڈیو یا کسی فلم کا ٹریلر چھوٹی سی ونڈو میں چل رہا ہوتا ہے اور چینل والا یا والی بڑی ونڈو میں خود موجود ہوتے ہیں اور اپنے تاثرات کو ریکارڈ کرتے ہیں۔ کئی لوگ تو وڈیو بناتے ہوئے باقاعدہ یہ بیان دیتے ہیں کہ میں نے ابھی تک اس وڈیو کو نہیں دیکھا اس لیے میرے تاثرات بالکل حقیقی ہوں گے۔ اب اگر وڈیو میں تاثرات دِکھانے والی کوئی خاتون ہے تو لاکھوں ویوز یقینی ہیں۔

اس سے اصل وڈیو بنانے والے کو بہت نقصان ہوتا ہے کیونکہ یہاں دیکھنے والے ایک ٹکٹ میں دو مزے لے اُڑتے ہیں، ایک تو وڈیو بھی دیکھ لی اور دوسرا تاثرات سے بھی لطف اندوز ہو لیے، اب بھلا اصل وڈیو جو کہ پہلے سے ہی دیکھ لی ہے اصل چینل پر دیکھنے کون جائے گا۔ مزیدار بات یہ ہے کہ کبھی کوئی ان ری ایکشن وڈیوز پر اپناری ایکشن دے تو یہ ناراض ہو جاتے ہیں بلکہ اُس وڈیو پر پھر اپناری ایکشن ریکارڈ کر دیتے ہیں یعنی کہ وڈیو کے اندر چلتی وڈیو میں بھی وڈیو اور پھر اُس کے آگے وڈیو میں بھی وڈیو۔ وڈیو نہ ہوگئی انسپشن (Inception) فلم ہوگئی کہ A dream within a dream within a dream?

جنسی کہانیاں

چند سال قبل جب جنسی کہانیاں کتابی صورت کی بجائے انٹرنیٹ پر آئیں تو انتہائی تیزی سے مقبول ہونا شروع ہوگئیں۔ لیکن پھر دنیا فیس بک اور یوٹیوب میں سمٹ گئی تو اس کی مقبولیت کم ہوگئی کیونکہ اب لوگ پڑھنے کی بجائے ''دیکھنے'' میں زیادہ دلچسپی لے رہے تھے۔ اب حال ہی میں یوٹیوب پر یہ سلسلہ دوبارہ سے زور پکڑ رہا ہے۔

انتہائی مخرب الاخلاق کہانیاں یوٹیوب پر ٹرینڈنگ میں نمبرون تک پہنچ جاتی ہیں اور ان کی کامیابی کا راز بھی زنانہ آواز ہے۔ زیادہ تر یہ کام ہندوستان میں ہو رہا ہے لیکن چونکہ ہندی اور اردو میں زیادہ فرق نہیں اس لیے پاکستان میں بھی یہ وڈیوز ٹرینڈنگ میں اوپر کے درجوں پر پہنچ جاتی ہیں۔

یہ سلسلہ یہیں نہیں رُکتا بلکہ وڈیوز کے نیچے تبصروں میں لوگ اپنے فون نمبرز بھی لکھنا شروع کر دیتے ہیں اور یوں جہلا کے سبب گند کا یہ سیلاب انٹرنیٹ کو اپنے دھارے میں بہائے لیے جاتا ہے۔

یوٹیوب پر فحش مواد بھلا کیسے اپ لوڈ ہو سکتا ہے؟

یوٹیوب پر ویسے تو فحش مواد سے نمٹنے کے لیے سخت قوانین موجود ہیں لیکن گوگل کی یہ سروس فحش وڈیوز سے بھرتی جا رہی ہے۔ یوٹیوب پر نہ صرف فحش

وڈیوز اپ لوڈ کی جا رہی ہیں بلکہ کاپی رائٹس کی خلاف ورزی بھی دھڑلے سے جاری ہے۔ یہ سب کچھ گوگل کے نظام میں موجود ایک چور دروازے کی وجہ سے ممکن ہو رہا ہے۔

دراصل یوٹیوب پر جب کوئی وڈیو اپ لوڈ کی جاتی ہے تو گوگل کی ہوسٹنگ سروس اسے کونٹینٹ آئی ڈی سافٹ ویئر کے ذریعے اسکین کرتی ہے۔ اسی دوران اس کا موازنہ کاپی رائٹ مواد سے بھی کیا جاتا ہے، اگر اس میں کوئی ایسی چیز موجود ہو تو اس وڈیو کو یوٹیوب پر جانے سے روک دیا جاتا ہے۔

لیکن اس پورے عمل سے وڈیو تبھی گزرتی ہے جب اسے عوامی طور پر یعنی Publically شیئر کیا جائے۔ جب کسی وڈیو کو پبلک کے لیے اپ لوڈ نہیں کیا جاتا تو یہ ویب سائٹ پر اپ لوڈ ہو جاتی ہے اور ایک چور دروازے سے دیکھنے کے لیے دستیاب بھی ہو جاتی ہے کیونکہ اب یہ فلٹر نہیں ہو گی۔

یہ وڈیو اب یوٹیوب پر تلاش کرنے سے تو نہیں ملے گی لیکن دیگر ویب سائٹس پر اسے یوٹیوب پلیئر کی مدد سے ایمبیڈ کیا جا سکتا ہے، یعنی وڈیو یوٹیوب پر موجود ہو گی، یوٹیوب پر دیکھی نہیں جا سکے گی لیکن دیگر ویب سائٹس پر با آسانی دیکھی جا سکتی ہے۔ اس کے علاوہ کاپی رائٹس کی خلاف ورزی کرتے ہوئے بھی مواد بڑی تعداد میں یوٹیوب پر اپ لوڈ کیا جا رہا ہے۔ اس حوالے سے کئی کمپنیز اپنے تحفظات کا اظہار کر چکی ہیں۔ ان کا کہنا ہے کہ ان کا مواد اس وقت تک یوٹیوب سے نہیں ہٹایا جاتا جب تک کوئی اسے رپورٹ نہ کرے اور رپورٹ کرنے پر بھی یوٹیوب کی جانب سے بہت دیر سے جواب دیا جاتا ہے۔

”موقعے پہ چوکا“ لگانے والے ماہر

بھئی اگر آپ یہ جاننا چاہتے ہیں کہ ”موقعے پہ چوکا“ کس طرح لگایا جاتا ہے تو یہ کام آپ با آسانی ماہرین کے یوٹیوب چینلز پر دیکھ سکتے ہیں۔ وہ اس طرح کے آج کل حالات جس دھارے میں بہہ رہے ہوں یا تازہ ترین کوئی بڑا واقعہ پیش آیا ہو تو فوراً اس حوالے سے کوئی ایسی وڈیو بنا دیں کہ لوگ دیکھنے پر مجبور ہو جائیں۔ یہ طریقہ بہت ہی آسان ہے۔

پچھلے دنوں جب پی آئی اے کی فلائٹ کے ساتھ حادثہ پیش آیا تو لوگوں نے اسے خوب کیش کرایا۔ کئی لوگوں نے جہاز کے اندر کے منظر کی وڈیوز پیش کر دیں جسے لاکھوں لوگ دیکھنے اُمڈ آئے۔ یہ سلسلہ چند دن تھما تو جنید جمشید مرحوم کی قبر سے خوشبوئیں پھوٹنے کا سلسلہ چل نکلا۔ کسی نے قبرستان کے گورکن کی وڈیو بنا دی جو کہہ رہا تھا کہ قبر سے خوشبوئیں پھوٹ رہی ہیں اور یہ ایک معجزہ ہے۔ ہماری قوم تو ویسے ہی معجزات کی دیوانی ہے اس لیے یہ وڈیو بھی ٹاپ ٹرینڈ میں پہنچ گئی۔

کسی شوبز یا سیاسی شخصیت کے ساتھ کوئی حادثہ پیش آ جائے بس کوئی سی بھی وڈیو چاہے وہ کاپی شدہ ہو فٹافٹ بے ہودہ سے عنوان کے ساتھ یوٹیوب پر ڈال دیں پھر دیکھیں لوگ کس طرح اسے دیوانہ وار دیکھتے ہیں۔ اس کی مثال وقار ذکا کے ساتھ پیش آئے تازہ ترین واقعے میں آپ دیکھ سکتے ہیں۔



حرفِ آخر

پہلے کہتے تھے کہ جاہل کا اُس وقت تک اندازا نہیں ہوتا جب تک وہ منہ نہیں کھولتا۔ لیکن اب کسی کے منہ کھلنے کا انتظار کیے بغیر کسی کی پروفائل سے اندازا لگایا جا سکتا ہے کہ وہ کتنے پانی میں ہے۔ اس لیے ہم وقتاً فوقتاً ایسے مضامین شائع کرتے رہتے ہیں کہ برائے مہربانی ایسے جعل سازوں سے دُور رہیں، یوٹیوب اور فیس بک پر ایسی چیزوں کی طرف مت جائیں جن میں آپ کی سیاسی، قومی یا مذہبی کمزوری کو استعمال کیا گیا ہو۔ چاہے کوئی عام بندہ ہو یا میڈیا ہاؤسز ان کا مقصد تو ویسے ہی آپ کو پھنسانا ہوتا ہے اس لیے وہ ایسی خبروں کی تلاش میں رہتے ہیں جن کو اپ لوڈ کر کے آپ کی توجہ حاصل کر سکیں۔ خدارا خود بھی ایسی چیزوں سے دُور رہیں اور دوسروں کو بھی آگاہ کریں تاکہ ہم ایک بہتر معاشرہ تعمیر کر سکیں۔

اسکیئر ویئر

ڈرانے دھمکانے والے کمپیوٹر پروگرام



وائرس یا مال ویئر کے حملوں سے بچنے کے بارے میں آپ کیا جانتے ہیں؟ عام صارفین کی بات کی جائے تو وہ اتنا جانتے ہیں کہ وائرس سے بچنے کے لیے غیر ضروری لنکس پر کلک نہ کیا جائے۔ کمپیوٹر ہو یا اسمارٹ فون یہ کلیہ دونوں جگہ کارآمد ہے۔ وائرس ایسی چیز ہے کہ کمپیوٹر اور فون استعمال کرنے والے ہمیشہ اس سے خوفزدہ رہتے ہیں اور اسی خوف کا فائدہ اُٹھاتے ہوئے وائرس بنانے والے انھیں مزید نشانہ بناتے ہیں۔

اسکیئر ویئر کیا ہے؟

یقیناً آپ سوچ رہے ہوں گے کہ خوف کے ذریعے کیسے کسی کے سسٹم یا موبائل فون پر حملہ کیا جاسکتا ہے؟ تو اس کا جواب یہ ہے کہ وائرس حملے کی ایک نئی شکل بھی کافی عرصے سے سامنے آچکی ہے اور اس کا نام ہے Scareware۔ جس طرح ایڈ ویئر اور مال ویئر ہوتے ہیں بالکل اسی طرح ''سکیئر ویئر'' بھی موجود ہے۔ فرق یہ ہے کہ ایڈ ویئر آپ کو اشتہارات دکھا کر پریشان کرتے ہیں جبکہ سکیئر ویئر میں آپ کو خوف زدہ کرنے کے بعد آپ کی ڈیوائس میں زبردستی مال ویئر منتقل کرنے کی کوشش کی جاتی ہے۔

دراصل اس میں یہ تکنیک استعمال کی جاتی ہے کہ صارف کو خوفزدہ کر کے اسے نشانہ بنایا جائے۔ جب سے اسمارٹ فون آئے ہیں یہ تکنیک مزید کامیابی کی جانب گامزن ہے۔ اس حملے میں صارف کو بتایا جاتا ہے کہ اس کا فون یا کمپیوٹر وائرس سے متاثر ہوچکا ہے، اگر وہ اسے صاف کرنا چاہتا ہے تو ہمارا سافٹ ویئر ڈاؤن لوڈ کرلے۔ اصل حملہ تو اس ڈاؤن لوڈنگ ربط پر کلک یا ٹچ کرنے کے بعد شروع ہوتا ہے کیونکہ یہی دراصل وائرس ہوتا ہے۔

حملے کا طریقہ کار

سکیئر ویئر کے حملے کا طریقہ کار بہت ہی سادہ لیکن انتہائی کارگر ہے اور تقریباً ہر اسمارٹ فون صارف اس کا ضرور سامنا کر چکا ہوتا ہے۔ اس میں کوئی ویب سائٹ دیکھتے ہوئے ایک پاپ اپ یا نئی ونڈو کھلتی ہے جو فون کو وائبریٹ کرتے ہوئے بتاتی ہے کہ آپ کے فون میں وائرس ہے، اگر آپ اسے صاف کرنا چاہتے

The page at andro-apps.com says:

*** ATTENTION ***
Your [blurred] is badly infected with (4) Virus!

The virus is stealing your personal data and slows your phone speed!

Follow the instructions to remove the virus immediately.

OK

android SECURITY

Your [blurred] may have (4) Virus!

You may have been infected with the virus while browsing insecure websites on **01 August, 2015.**

WARNING ! Your private photos, Facebook data, passwords and information about your credit card are at risk.

How to remove virus :
Step 1: Tap the button and install "360 Security - Antivirus Boost" for free on Google Playstore

Step 2:Open the app and remove all virus now!

Confirm Navigation

!! WARNING !!

Your phone is exposed to HIGH RISK and UNSECURED.

If you do not have warranty, any damage to your phone cannot be fixed.

Click *Stay on page* and download recommended app to fix your phone now!

Are you sure that you want to leave this page?

Stay on this Page | Leave this Page

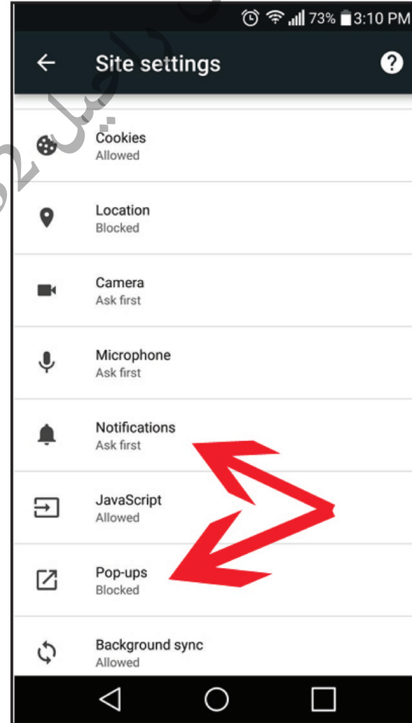
Step 2:Open the app and remove all virus n

ہیں تو فلاں آپشن کا استعمال کریں، یعنی دراصل اصلی مال ویئر کو فون میں ڈاؤن لوڈ کرلیں۔

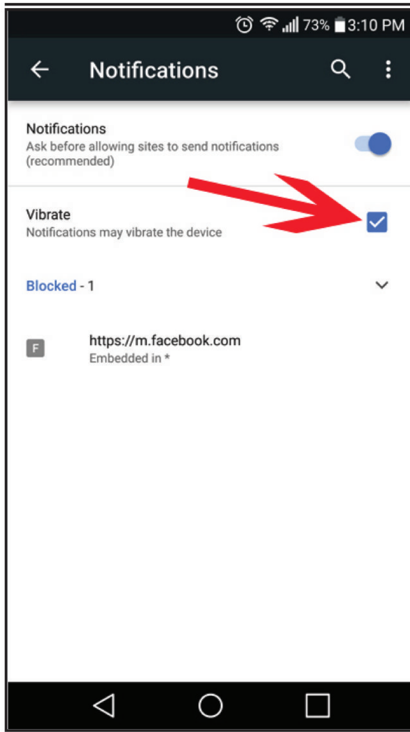
پاپ اپ فون وائبریٹ کیسے کرتا ہے؟

اسمارٹ فون صارفین کو مزید خوف زدہ کرنے کے لیے اس کے وائبریٹ فیچر کو استعمال کیا جاتا ہے۔ گوگل کروم براؤزر میں پہلے سے فون کو وائبریٹ کرنے کی اجازت دی گئی ہوتی ہے اور عام اسمارٹ فون صارفین جو کسی بھی ایپ کی نوٹی فلکیشنز سیٹنگز میں جھانکتے تک نہیں وہ باآسانی اس تکنیک سے خوفزدہ ہو جاتے ہیں۔۔ اگر آپ گوگل کروم کی نوٹی فکیشن سیٹنگز دیکھیں تو آپ کو معلوم ہو گا کہ آپ نے اسے فون کو وائبریٹ کرنے کی اجازت دے رکھی ہے۔

اس طرح وائرس پھیلانے والی ویب سائٹس کروم کی وائبریشن اے پی آئی (Vibration API) کو استعمال کرتے ہوئے اپنے پاپ اپ کے ذریعے آپ کے فون کو جھنجوڑ کر رکھ دیتی ہیں۔ اس سے صارف یہ سمجھتا ہے کہ ضرور اس کے فون میں وائرس آ چکا ہے اس لیے اب اس کی صفائی انتہائی ضروری ہے۔ اسی خوف کی وجہ سے وہ وائرس کا نشانہ بنتا ہے حالانکہ اس سے قبل تو اسے صرف ڈرایا گیا ہوتا ہے وائرس ابھی سسٹم میں نہیں پہنچتا۔



یہاں یہ بات سمجھنے کی انتہائی اشد ضرورت ہے کہ یہ وائبریشن پر مشتمل الرٹ نہ تو وائرس دِکھاتا ہے اور نہ ہی آپ کا آپریٹنگ سسٹم آپ کو تنبیہ کر رہا ہوتا ہے یہ صرف اور صرف ایک نوٹی فکیشن کا کمال ہے۔



یہ ایک انتہائی اہم معاملہ ہے اور آج کل اینڈرائیڈ استعمال کرنے والی بڑی تعداد اس سے پریشان ہے، اس لیے جب تک براؤزر اس کا بندوبست نہیں کرتا آپ خود اس کی سیٹنگز میں جا کر وائبریشن نوٹی فکیشنز اور پاپ اپس کو بند کردیں۔

چونکہ اینڈرائیڈ میں گوگل کروم براؤزر پہلے سے ہی موجود ہوتا ہے اس لیے زیادہ تر اینڈرائیڈ صارفین اسے ہی استعمال کرتے ہیں۔ ان غیرضروری چیزوں کو کروم میں بند کرنے کے لیے براؤزر کھولیں اور سیٹنگز کے اندر موجود ''سائٹ سیٹنگز'' میں آجائیں۔ یہاں پاپ اپ اور وائبریشن نوٹی فلکیشنز کو بند کرنے کا آپشن موجود ہوگا۔

سکیئر ویئر حملوں کا مقصد کیا ہے؟

سکیئر ویئر حملوں کا مقصد بھولے بھالے صارفین سے پیسے ہتھیانا ہے۔ اگر آپ غلطی سے اس کے چکمے میں آنے کے بعد وائرس صاف کرنے کے لیے اس کے لنک پر کلک کر بیٹھیں تو اس کا جعلی اسکینر فوراً حاضر ہو کر آپ کا سسٹم یا ڈیوائس اسکین کرنا شروع کر دیتا ہے۔ اس کے بعد وہ ایک جعلی رپورٹ بھی پیش کرتا ہے کہ فلاں فلاں وائرسز آپ کے سسٹم میں دریافت کر لیے گئے ہیں اور اگر آپ انھیں صاف کرنا چاہتے ہیں تو یہ سہولت آپ کو ہمارے مفت پروگرام میں نہیں ملے گی بلکہ اب اس کا پروفیشنل ورژن خریدنا ہوگا۔

اگر کوئی ان کے جال میں پھنس جائے تو ظاہر ہے اس کی رقم ضائع ہی ہوتی ہے، اس کے بعد یہ پلٹ کر خبر بھی نہیں لیتے۔ اگر خوش قسمتی سے ہیکر کوئی نیک دل انسان ہو تو صرف سافٹ ویئر کے عوض ادا کی گئی رقم پر ہی اکتفا کر لیتا ہے لیکن اگر اس کا ارادہ ایک ہی بندے سے سارے دن کی کمائی جمع کرنا ہو تو وہ دی گئی کریڈٹ کارڈ کی تفصیلات کو استعمال کرتے ہوئے مزید مالی نقصان بھی پہنچا سکتا ہے۔

اس حملے کی صورت میں کیا کرنا چاہیے؟

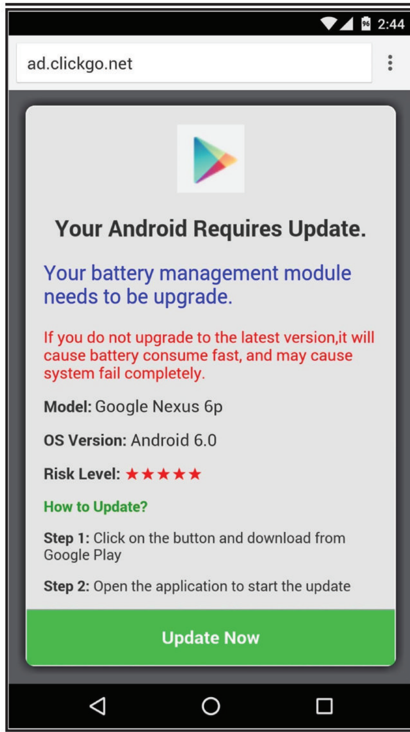
جیسا کہ ہم نے پہلے ذکر کیا کہ یہ بہت ہی عام صورتِ حال ہے۔ اگر آج تک آپ کو ایسا کوئی اتفاق نہیں ہوا تو مستقبل میں ضرور ہو سکتا ہے اس لیے یہ بات یاد رکھیں کہ کوئی بھی پاپ آپ کے سسٹم یا فون میں کوئی فائل منتقل نہیں کر سکتا اور نہ کوئی سافٹ ویئر یا ایپلی کیشن انسٹال کر سکتا ہے۔

اگر یہ پاپ اپ آپ کے سامنے آیا ہے اور آپ کا فون وائبریٹ بھی ہوا ہے تو اس کا یہ مطلب نہیں ہے کہ وائرس ڈیوائس میں منتقل ہو چکا ہے۔ اس لیے اپنے حواس قابو میں رکھیں کیونکہ اس حملے میں پاپ اپ کی ایک لہر آتی ہے اور وہ کھلتے چلے جاتے ہیں۔ اس لیے فون پر اس حملے کے دوران فوراً ہوم بٹن پر کلک کرتے ہوئے تمام ایپس کو منی مائز کرنے کے بعد سب کو بند کر دیں۔

حفاظتی تدابیر

وائرسز سے بچنے کے لیے اپنے فون اور کمپیوٹر میں اینٹی وائرس کی انسٹالیشن یقینی بنائیں۔ اینٹی وائرس کوئی سا بھی ہو اس کا اپ ڈیٹ ہونا انتہائی ضروری ہوتا ہے تا کہ وہ نت نئے حملوں سے آگاہ ہو۔ کمپیوٹر و اسمارٹ فون کے لیے کئی اینٹی وائرس پروگرام مفت دستیاب ہیں، آپ اپنی پسند سے انھیں تلاش کر کے اور دوسروں کی اس کے بارے میں رائے پڑھنے کے بعد اسے انسٹال کر لیں۔ سب سے اہم حفاظتی تدبیر یہ ہے کہ اپنے تجسس پر قابو رکھیں اور سوشل میڈیا پر ڈالے گئے غیر مصدقہ ذرائع کے روابط پر بالکل بھی کلک مت کریں۔

ایپلی کیشنز و اینڈرائیڈ کے جعلی اپ ڈیٹ پیغامات کو بھی ہمیشہ نظر انداز کر دیں۔ مثلاً وٹس ایپ وغیرہ کے نئے فیچرز آنے سے قبل ہی خبروں میں آ چکے



ہوتے ہیں اور سبھی صارفین انھیں حاصل کرنا چاہتے ہیں۔ ہیکرز اسی چیز کا فائدہ اُٹھاتے ہوئے پیغامات پھیلاتے ہیں کہ اس لنک سے آپ وٹس ایپ یا فلاں ایپ کا نیا ورژن ڈاؤن لوڈ کر سکتے ہیں۔ اس کے علاوہ صارفین اینڈرائیڈ کو بھی اپ گریڈ کرنے کے شوقین ہوتے ہیں اور اس حوالے سے پیغامات انھیں موصول ہوتے رہتے ہیں۔ اس لیے ایسے تمام پیغامات پر بالکل بھی توجہ مت دیں۔ جب کوئی ایپلی کیشن اپ ڈیٹ ہو گی تو آفیشیل طریقہ کار سے آپ کے پاس بھی اپ ڈیٹ کا نوٹی فکیشن آ جائے گا یا ایپ خود بخود اپ گریڈ ہو جائے گی۔ اسی طرح اینڈرائیڈ کی اپ ڈیٹ بھی اپنے فون بنانے والی کمپنی کی طرف سے آنے کا انتظار کریں، ورنہ جلد بازی آپ کو نقصان پہنچا سکتی ہے۔

یاد رکھیں کہ اسکیئر ویئر تکنیک کو استعمال کرتے ہوئے آپ پر رینسم ویئر (Ransomware) حملہ بھی ہو سکتا ہے۔ رینسم ویئر میں آپ کی ڈرائیو میں موجود تمام فائلز کو انکرپٹ کر دیا جاتا ہے اور آپ انھیں استعمال نہیں کر پاتے۔ اگر آپ اپنی قیمتی فائلز واپس حاصل کرنا چاہتے ہیں تو اس کے لیے تاوان ادا کرنا پڑتا ہے جس کے بعد آپ کو وہ سافٹ ویئر فراہم کیا جاتا ہے جو ان فائلز کو دوبارہ استعمال کے قابل بناتا ہے۔ اس حملے کی صورت میں صارف کو ہر حال میں تاوان ادا کرنا ہی پڑتا ہے کیونکہ اِنکرپٹ کردہ فائلز کو کسی صورت بھی کسی دوسرے پروگرام سے ڈی کرپٹ نہیں کیا جا سکتا اور اس کے بغیر فائلز استعمال کے قابل بھی نہیں رہتیں۔



اسمارٹ فون میں ایک ساتھ دو کیمروں کے بارے میں اہم باتیں

آج کل اسمارٹ آج فونز میں اتنے اچھے کیمرے آنے لگے ہیں کہ انہوں نے ڈیجیٹل کیمروں کا زمانہ تقریباً ختم کر دیا ہے۔ اسمارٹ فون بنانے والی کمپنیوں کے سامنے چیلنج یہ ہوتا ہے کہ وزن اور موٹائی کم رکھتے ہوئے کس طرح کیمروں کو بہتر بنایا جائے۔ اس مسئلے کو دُور کرنے کے لئے اب ایک ہی ڈیوائس میں زیادہ کیمرے لگائے جا رہے ہیں۔ اگر فون میں سامنے یا پیچھے کی جانب ایک ساتھ دو کیمرے موجود ہوں تو اس کے کیا فوائد ہو سکتے ہیں؟ آیئے آپ کو بتاتے ہیں۔

دُہرا کیمرا آخر ہے کیا؟

اسمارٹ فون کی بیک سائیڈ میں ایک چھوٹا سا کیمرا لینس دیا گیا ہوتا ہے۔ اسمارٹ فونز میں کیمرہ ماڈیول کافی چھوٹا ہے، کیونکہ فون خود بھی پتلا ہوتا ہے۔ اس مختصر ماڈیول کے اندر ہی لینس کے کئی عناصر کو ڈالنا ہوتا ہے۔ ان میں امیج سینسر اور آپٹیکل امیج اسٹیبلائزیشن کے لئے چھوٹی موٹرز بھی ہوتی ہیں۔

دُہرے کیمرے سیٹ اپ میں آپ کو دو لینس نظر آئیں گے، جنہیں ایک ساتھ دائیں بائیں یا اوپر نیچے لگایا گیا ہوتا ہے۔ اس کا مطلب ہے کہ آلے میں دو پلیٹ اور الگ الگ کیمرہ ماڈیول لگے ہیں۔ ان میں سے ایک پرائمری لینس ہوتا ہے، جو بنیادی کام کرتا ہے۔ دوسرا اضافی روشنی، گہرائی، فوکس کی گئی چیز کے اردگرد اور بیک گراؤنڈ کو بلر کرنے جیسے کام انجام دیتا ہے۔

دُہرے کیمرے والا پہلا فون

دُہرے کیمرے والا اسمارٹ فون سب سے پہلے سال 2011 میں دیکھنے کو ملا تھا۔ HTC Evo 3D اسمارٹ فون میں دُہرا کیمرا سیٹ اپ استعمال کیا گیا تھا تاکہ 3D فوٹو لی جا سکیں۔ انہیں اسمارٹ فون کی 3D سکرین پر دیکھا جا سکتا تھا۔ اس کے بعد اس ٹیکنالوجی کے ساتھ تجربات کیے جاتے رہے، مگر خیال کامیاب نہیں ہوا۔ سال 2014 میں HTC One M8 میں دُہرا کیمرا سیٹ اپ لگا ہوا تھا۔ یہ کافی شاندار نتائج دے رہا تھا۔

2016 میں دُہرے کیمروں نے اسمارٹ فونز میں جگہ کی پریشانی کو دُور کرتے ہوئے شاندار رزلٹ دینا شروع کر دیا۔

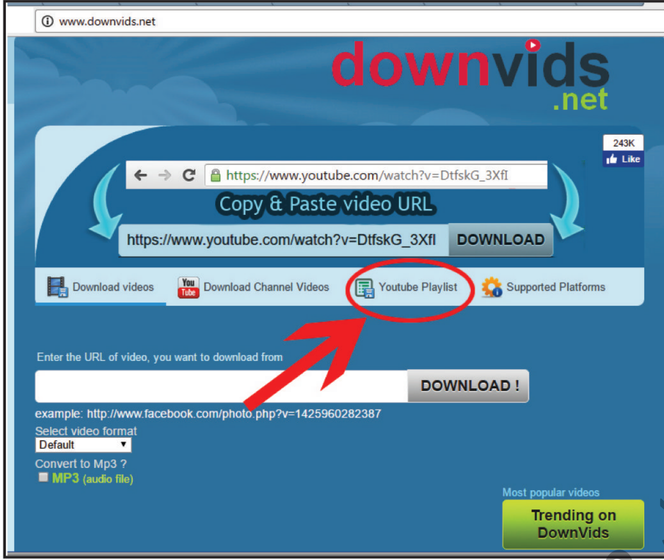
دُہرے کیمرے کے نظام کا فائدہ کیا ہے؟

اس حوالے سے دماغ میں سوال اُبھرتے ہیں کہ دُہرے کیمرے سیٹ اپ میں دوسرے کیمرے کو کس طرح استعمال کیا گیا ہے، اس کی وجہ سے تصاویر کا رزلٹ کیسا ہے؟ دُہرے کیمرے سے بنائی گئی تصویر واحد کیمرے کے مقابلے میں بہت زیادہ تفصیلات کی حامل ہوتی ہے۔ اس میں فوکس انتہائی عمدہ ہوتا ہے اور تصویر میں رنگ انتہائی نمایاں ہوتے ہیں۔ کئی بار دُہرے کیمرے سے 1x اور 2x آپٹیکل زوم میں اضافہ کرنے میں بھی مدد ملتی ہے۔

تصویر کا معیار کئی باتوں پر منحصر ہوتا ہے

اگرچہ دُہرے کیمرے سے نتائج اچھے آئیں، مگر سینسر سائز، پکسلز سائز، اپرچر اور پوسٹ پروسیسنگ بھی اچھی تصاویر کھینچنے میں اہم کردار ادا کرتے ہیں۔ ایسا نہیں ہے کہ کوئی عام سا دُہرے کیمرے والا فون آپ کو انتہائی اعلیٰ معیار کی تصاویر بنا کر دے۔ سام سنگ گلیکسی S7 / S7 Edge، گوگل پکسلز، ون پلس 3، LG G5 اور HTC 10 مختصر روشنی میں بہت سے دُہرے کیمرے والے اسمارٹ فونز کے مقابلے اچھی تصاویر لیتے ہیں۔

پوری یوٹیوب پلے لسٹ ڈاؤن لوڈ کریں بغیر کسی سافٹ ویئر کے

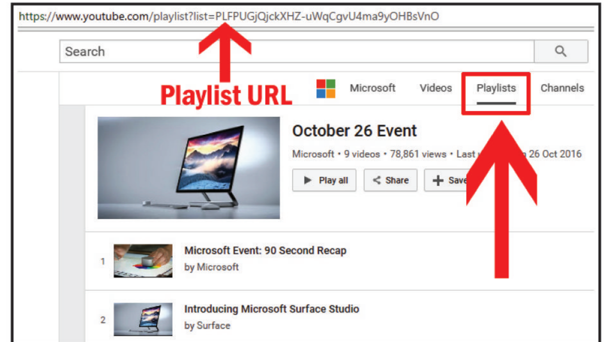


ویڈیوز ڈاؤن لوڈ کرنا سبھی کا پسندیدہ مشغلہ ہے اور اس حوالے سے سبھی کی کوشش ہوتی ہے کہ کوئی آسان ترین طریقہ معلوم ہو۔ زیادہ تر ویڈیوز ڈاؤن لوڈ کرنے کے لیے کسی نہ کسی سافٹ ویئر یا ایپلی کیشن کی ضرورت ہوتی ہے لیکن ایسے بھی کئی طریقے موجود ہیں جن سے کسی سافٹ ویئر کے بغیر بھی ویڈیوز ڈاؤن لوڈ کی جاسکتی ہیں۔ ایک آدھ ویڈیو ڈاؤن لوڈ کرنا تو آسان ہے آیئے آپ کو بتاتے ہیں کہ کس طرح یوٹیوب کی ایک پوری کی پوری پلے لسٹ ڈاؤن لوڈ کی جاسکتی ہے۔

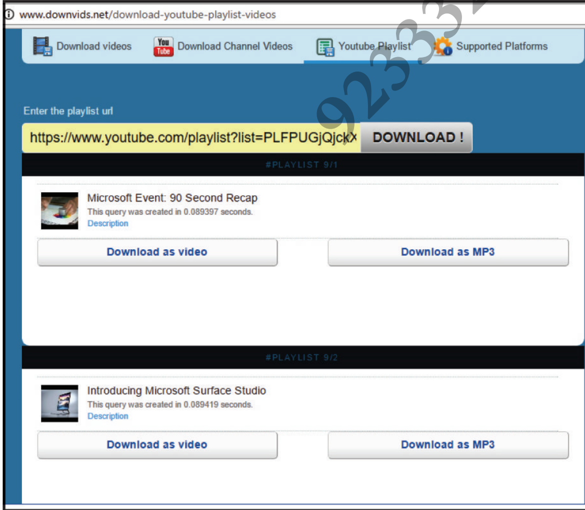
یوٹیوب پر ویڈیوز کو فہرست میں مرتب رکھنے کے لیے پلے لسٹس بنائی جاتی ہیں، مثلاً کسی ایک خاص موضوع پر موجود ویڈیوز کو ایک سیکشن میں جمع کرنے کے لیے اس کی پلے لسٹ بنادی جاتی ہے۔ اب اگر آپ کسی پلے لسٹ میں موجود تمام ویڈیوز ڈاؤن لوڈ کرنا چاہتے ہیں تو یہ کام بہت ہی آسانی کے ساتھ ''ڈاؤن وِڈز ڈاٹ نیٹ'' ویب سائٹ کے ذریعے کیا جاسکتا ہے:

www.downvids.net

اس ویب سائٹ کے ذریعے آپ ایک ویڈیو بھی ڈاؤن لوڈ کرسکتے ہیں اور پوری پلے لسٹ بھی۔ پلے لسٹ کو ڈاؤن لوڈ کرنے کے لیے یہاں دیکھیں ''یوٹیوب پلے لسٹ'' کا آپشن موجود ہے۔ سب سے پہلے یوٹیوب سے اپنی مطلوبہ پلے لسٹ کا ربط کاپی کرلیں۔



پلے لسٹ کا یوآرایل پیسٹ کرنے کے بعد ''سلیکٹ ویڈیو فارمیٹ'' میں سے مطلوبہ فارمیٹ جیسے کہ عام یا ایچ ڈی منتخب کرنے کے بعد ڈاؤن لوڈ کے بٹن پر کلک کردیں۔ اس پلے لسٹ میں موجود تمام ویڈیوز اگلے صفحے پر ڈاؤن لوڈ کرنے کے لیے موجود ہوں گی۔



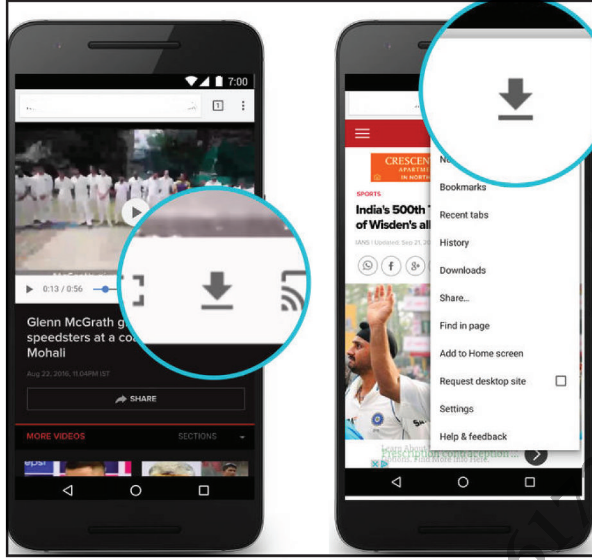
اس سروس سے آپ ویڈیوز کو ایچ ڈی معیار میں یا صرف بطور ایم پی تھری بھی کنورٹ کرکے ڈاؤن لوڈ کرسکتے ہیں۔

وڈیوز، تصاویر اور گانے ڈاؤن لوڈ کرنے کے لیے کروم کا نیا فیچر

انٹرنیٹ پر موجود مواد کو ڈاؤن لوڈ کرنا ایک بڑی سہولت ہے۔ اس طرح بار بار اس کا مطالعہ کرنے کے لیے انٹرنیٹ کی ضرورت نہیں رہتی اور جب چاہیں اسے آف لائن رہتے ہوئے بھی دیکھا جا سکتا ہے۔ کمپیوٹر استعمال کرتے ہوئے تو یہ کام کافی آسان ہے لیکن اسمارٹ فون پر اس کے لیے کافی پاپڑ بیلنا پڑتے ہیں۔ تاہم گوگل نے اب اپنے صارفین کی یہ مشکل آسان کرنے کا فیصلہ کر لیا ہے۔ کچھ ہی عرصہ پہلا گوگل نے یوٹیوب کی اسمارٹ فون ایپلی کیشن میں یہ فیچر مہیا کیا تھا کہ کسی بھی وڈیو کو آف لائن دیکھنے کے لیے محفوظ کیا جا سکتا ہے۔

اب گوگل نے ایک قدم مزید آگے بڑھاتے ہوئے اسمارٹ فون کے لیے دستیاب کروم کے ورژن 55 میں ڈاؤن لوڈنگ کا فیچر مہیا کر دیا ہے۔ اس کی بدولت آپ نہ صرف وڈیوز بلکہ ویب پیجز کو بھی آف لائن دیکھنے کے لیے ڈاؤن لوڈ کر سکتے ہیں۔

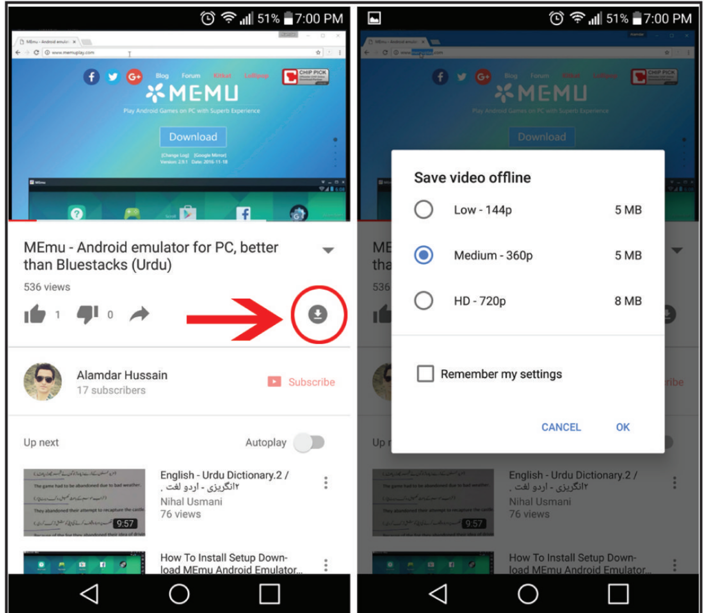
کسی ویب سائٹ پر موجود کوئی تحریر اگر آپ بعد میں کسی وقت پڑھنا چاہتے ہوں تو اس فیچر کی بدولت آپ اسے آف لائن دیکھنے کے لیے ڈاؤن لوڈ کر سکتے ہیں۔ اس کے لیے اگر آپ کے پاس کروم کا ورژن 55 انسٹال ہے تو مینو میں ''ڈاؤن لوڈ'' کا بٹن موجود ہوگا۔ اسی طرح اگر آپ فون پر کوئی وڈیو دیکھ رہے



ہوں گے تو اس کے ساتھ بھی ڈاؤن لوڈ بٹن ظاہر ہو جائے گا۔

اگر آپ کے پاس یہ بٹن دکھائی نہ دے تو گوگل پلے اسٹور سے کروم کا ورژن اپ ڈیٹ کر لیں۔ اس فیچر کے ذریعے آپ ویب پیجز کے علاوہ وڈیوز، میوزک اور تصویروں کو بھی با آسانی ڈاؤن لوڈ کر سکیں گے۔ آف لائن دیکھنے کے لیے ڈاؤن لوڈ کیا گیا آپ کا تمام مواد کروم میں ایک الگ حصے میں موجود رہے گا اور آپ جب چاہیں اسے ملاحظہ کر سکیں گے۔

یہی نہیں گوگل نے کروم کے نئے ورژن میں مزید بہتریاں بھی لائی ہیں مثلاً اب اس کی کارکردگی گزشتہ ورژنز کے مقابلے میں کہیں بہتر ہے، یہ میموری کا بھی کم استعمال کرتا ہے اور چلتے وقت کافی مستحکم رہتا ہے۔ اس میں اب ای میلز اور پیغامات لکھتے ہوئے الفاظ کے غلط اسپیلنگ کی نشاندہی بھی کی جائے گی۔



کمزور سسٹم پر بھی اینڈرائیڈ استعمال کریں بغیر کسی مسئلے کے

اینڈرائیڈ آپریٹنگ سسٹم کو ایمولیٹر کے ذریعے کمپیوٹر پر استعمال کرنا ہمارے ہاں کافی پسند کیا جاتا ہے۔ چونکہ ان پر اینڈرائیڈ کے گیمز کھیلے جا سکتے ہیں اور ایپلی کیشنز بھی استعمال کی جاسکتی ہیں اس لیے کمپیوٹر کی سہولت اور بڑی اسکرین پر اس کا مزہ دوبالا ہو جاتا ہے، گویا کمپیوٹر پر ایک اینڈرائیڈ ٹیبلٹ حاصل ہو جاتا ہے۔ اس میں کمپیوٹر پر چلنے والا انٹرنیٹ بھی چل رہا ہوتا ہے اور ماؤس کا کی بورڈ ماؤس بھی تو اس کو استعمال کرنا اور زیادہ آسان ہو جاتا ہے۔

زیادہ تر لوگ انھیں اس لیے بھی استعمال کرتے ہیں کہ ان میں اینڈرائیڈ کے گیمز کے علاوہ ایپلی کیشنز بھی انسٹال ہو جاتی ہیں جیسے کہ وٹس ایپ وغیرہ۔ اس طرح اگر آپ کے پاس ایک سے زائد فون نمبر موجود ہیں تو ایک نمبر پی سی پر موجود وٹس ایپ میں بھی استعمال کیا جاسکتا ہے۔

اس وقت کئی اینڈرائیڈ ایمولیٹر موجود ہیں جن میں سے بلیو اسٹیکس سب سے زیادہ معروف ہے۔ اس کے علاوہ ہم کمپیوٹنگ میں ''کو پلیئر'' اور ''Memu'' کے بارے میں بھی جائزہ شائع کر چکے ہیں جن کو اس مقصد کے لیے استعمال کیا جا سکتا ہے۔ ان تمام اینڈرائیڈ ایمولیٹرز کے بارے میں قارئین شکایت کرتے ہیں کہ یہ بہت زیادہ ہارڈ ویئر طلب کرتے ہیں اور ان کے کمپیوٹرز پر یہ ہینگ ہو جاتے ہیں۔ اگر آپ بھی اس صورتِ حال سے دوچار ہیں تو آپ کو ''نوکس ایپ پلیئر'' (Nox App Player) استعمال کرنا چاہیے۔ اس کی خاصیت یہ ہے کہ یہ کم ہارڈ ویئر کے حامل X86/AMD سسٹمز پر بھی باآسانی اور برق رفتاری سے کام کرتا ہے۔ نوکس اس وقت اینڈرائیڈ کے ورژن 4.4.2 پر مبنی ہے اور اسے آپ ونڈوز کے علاوہ میک پر بھی استعمال کر سکتے ہیں۔ اس کے چند اہم فیچرز درج ذیل ہیں:

اس میں گوگل پلے اسٹور پہلے سے موجود ہے۔

نوکس پلیئر کو ملٹی ونڈوز میں بھی استعمال کیا جاسکتا ہے۔



اگر آپ کے پاس APK فائلز موجود ہوں تو انھیں اس پر ڈریگ اینڈ ڈراپ کے ذریعے بھی انسٹال کیا جاسکتا ہے۔

نوکس پلیئر پر سی پی یو، ریم اور ریزولوشن کو کسٹمائز کرنے کی سہولت بھی موجود ہے جبکہ اس جیسا کوئی دوسرا پروگرام یہ آپشن نہیں دیتا۔

نوکس کا ڈیٹا باآسانی کمپیوٹر میں بیک اپ کیا جاسکتا ہے۔

اس میں روٹ کو آن آف کرنے کا بٹن بھی موجود ہے۔ یعنی جب چاہیں روٹ شدہ اینڈرائیڈ استعمال کیا جاسکتا ہے۔

اسکرین شاٹ کے علاوہ اس کے ذریعے اسکرین کی وڈیو ریکارڈنگ بھی کی جا سکتی ہے۔

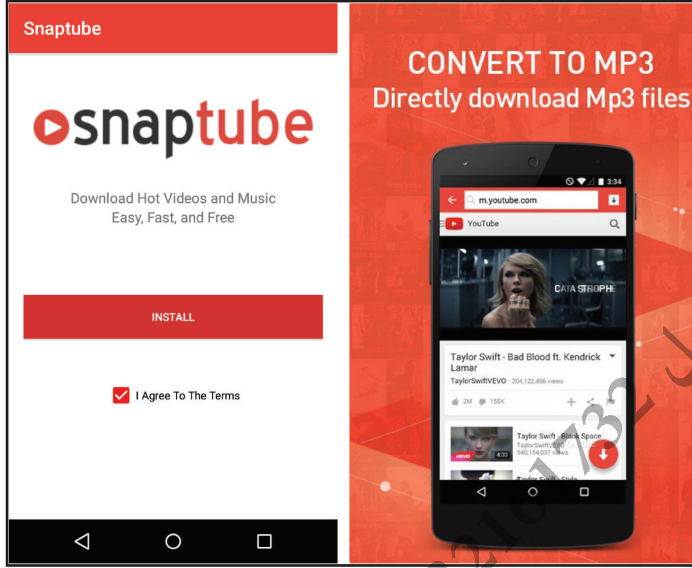
www.bignox.com



کسی بھی ویب سائٹ سے وڈیوز فون میں ڈاؤن لوڈ کریں

اگر آپ اسمارٹ فون پر وڈیوز ڈاؤن لوڈ کرنا پسند کرتے ہیں تو اس کے لیے ہم ایسی کئی ایپلی کیشنز کا تجزیہ کمپیوٹنگ میں شائع کر چکے ہیں جیسے کہ ٹیوب میٹ اور وِڈمیٹ وغیرہ۔ لیکن کسی بھی کام کے لیے کبھی بھی صرف ایک ایپلی کیشن پر اکتفا نہیں کرنا چاہیے بلکہ اس کے متبادل ذرائع کا بھی معلوم ہونا ضروری ہے۔ اس لیے اس بار ہم ایک اور ایپلی کیشن کے لیے پیش کر رہے ہیں جس کا نام ''اسنیپ ٹیوب'' (SnapTube) ہے۔ اس ایپلی کیشن کو استعمال کرتے ہوئے آپ یوٹیوب اور فیس بک سمیت 30 سے زائد ویب سائٹس سے وڈیوز براہِ راست اپنے فون میں ڈاؤن لوڈ کر سکتے ہیں۔

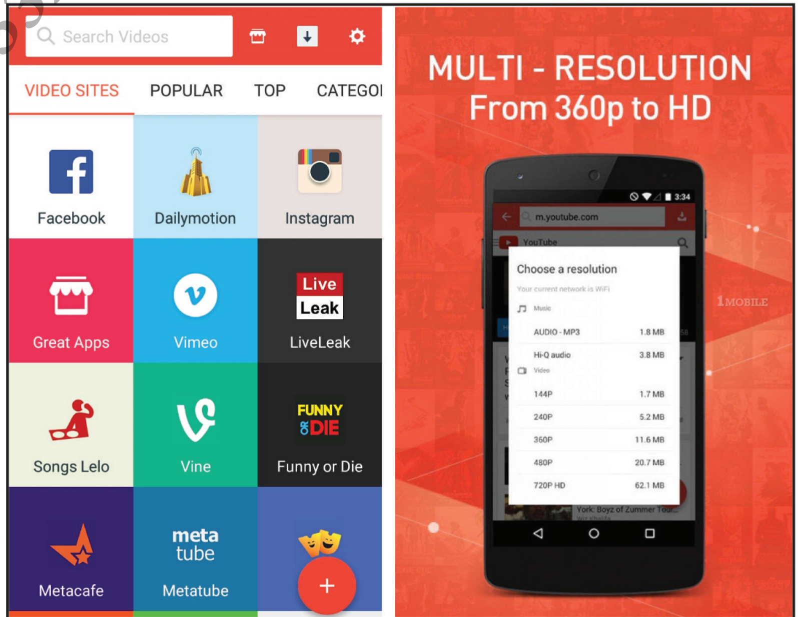
اگر کسی وڈیو کا لنک آپ کے پاس موجود ہے تو اسے براہِ راست لنک کے ذریعے ڈاؤن لوڈ کیا جا سکتا ہے لیکن اگر آپ ویسے ہی وڈیوز تلاش کر کے ڈاؤن لوڈ کرنا چاہتے ہیں تو اس کا بندوبست بھی موجود ہے یعنی آپ کی ورڈز سے بھی وڈیوز کو تلاش اور پھر ڈاؤن لوڈ کر سکتے ہیں۔ وڈیوز ڈاؤن لوڈ کرتے ہوئے آپ اپنی پسند کی کوالٹی منتخب کر سکتے ہیں۔ اگر وڈیو ایچ ڈی کوالٹی میں موجود ہو تو اسے 1080p میں بھی ڈاؤن لوڈ کر سکتے ہیں اور چاہیں تو اس میں موجود صرف میوزک کو MP3 فارمیٹ میں ڈاؤن لوڈ کر



سکتے ہیں، یعنی اسمارٹ فون پر وڈیوز ڈاؤن لوڈ کو اپنی پسند کے معیار اور پسند کے فارمیٹ میں ڈاؤن لوڈ کرنے کا مکمل بندوبست اس ایپ میں موجود ہے۔

چونکہ یہ ایپلی کیشن گوگل کے قوانین سے مطابق نہیں رکھتی اس لیے یہ آپ کو گوگل پلے اسٹور پر نہیں ملے، اس کی apk فائل ڈاؤن لوڈ کر کے انسٹالیشن کرنا ہوگی۔ اس ایپ کو بنانے والوں نے اس بات کی یقین دہانی کرائی ہے کہ اس میں کسی قسم کا کوئی سکیوریٹی خطرہ موجود نہیں اور اسے آپ بے فکر ہو کر ڈاؤن لوڈ کر کے انسٹال کر سکتے ہیں۔ اس کے لیے اس کی ویب سائٹ ملاحظہ کیجیے:

www.snaptubeapp.com



فون سے ڈیٹا اس طرح حذف کریں کہ کوئی ریکور نہ کر سکے

کمپیوٹنگ میں ہم اس سے پہلے بھی کئی دفعہ ذکر کر چکے ہیں کہ اپنا فون کسی دوسرے کو مستقل بنیادوں پر دینے یا بیچنے سے قبل اس میں موجود تمام ڈیٹا کو اچھی طرح حذف ضرور کر دیں۔ دراصل جو ڈیٹا آپ حذف یعنی ڈیلیٹ کرتے ہیں وہ بدستور ڈرائیو پر موجود رہتا ہے اور اسے بعد میں ریکور بھی کیا جا سکتا ہے۔ ہمارا انتہائی حساس ڈیٹا ہمارے فون میں موجود رہتا ہے اس صورت میں یہ کسی طرح سے دانشمندی نہیں کہ آپ اس بات کو یقینی بنائے بغیر کہ اب ڈیٹا ریکور نہیں کیا جا سکتا، فون کسی دوسرے کے حوالے کر دیں۔ عام طور پر لوگ فون میں موجود تمام ڈیٹا کو ایک ساتھ ختم کرنے کے لیے فیکٹری ری سیٹ کے آپشن کا استعمال کرتے ہیں لیکن یہ مسئلے کا حل نہیں، کیونکہ اس کے باوجود ڈیٹا ریکوری کے لیے موجود رہتا ہے۔ اس لیے اگر آپ اس کام کو آسان بنانا چاہتے ہیں تو سافٹ ویئر کمپنی ''ونڈر شیئر'' کا بنایا ہوا پروگرام ''سیف ایریزر'' (Wondershare SafeEraser) استعمال کر سکتے ہیں۔ یہ پروگرام آپ کو کئی سہولتیں دیتا ہے آیئے اس کی تفصیل آپ کو بتاتے ہیں۔

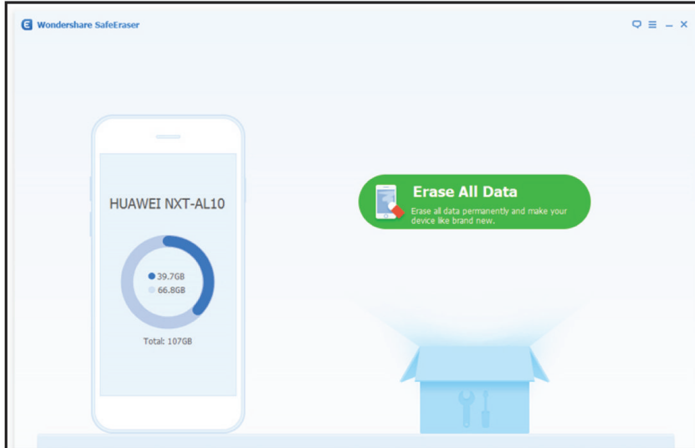
ایسا نہیں کہ یہ براہِ راست فون میں موجود تمام ڈیٹا حذف کرنا شروع کر دیتا ہے بلکہ آپ اسے فون سے صرف فالتو فائلز کو حذف کرنے کے لیے یعنی فون کلین اپ کے لیے بھی استعمال کر سکتے ہیں۔ اس کے لیے یہ صرف آپ کی پہلے سے ڈیلیٹ شدہ فائلوں کو ہی حذف کر کے خالی اسپیس بنا دیتا ہے۔

اگر آپ مستقل بنیادوں پر فون میں موجود تمام ڈیٹا ٹھکانے لگانا چاہتے ہیں تو یہ کام بھی اس پروگرام سے انجام دیا جا سکتا ہے لیکن اس سے قبل اپنے فون کا بیک اپ ضرور بنا لیں تا کہ بعد میں پچھتانا نہ پڑے۔ سیف ایریزر صرف میڈیا یا فائلز تک محدود نہیں بلکہ یہ فون میں موجود ہر طرح کا ڈیٹا جیسے کہ کال لاگز، ایس ایم ایس، کیلنڈر اور دیگر ہر طرح کے ذاتی ڈیٹا کو اس طرح حذف کر سکتا ہے کہ بعد میں اسے ریکور نہ کیا جا سکے۔ اس کام کے لیے یہ پروگرام تین مختلف طریقے پیش کرتا ہے، جن میں آپ کے ڈیٹا کے اوپر فرضی ڈیٹا اوور رائٹ کیا جاتا ہے تا کہ ریکوری کی کوشش میں آپ کا اصل ڈیٹا ہاتھ نہ لگے۔



اینڈرائیڈ و آئی او ایس دونوں کے لیے یہ پروگرام بذریعہ کمپیوٹر کام کرتا ہے اور آپ اسے ونڈوز و میک کے لیے ڈاؤن لوڈ کر سکتے ہیں:

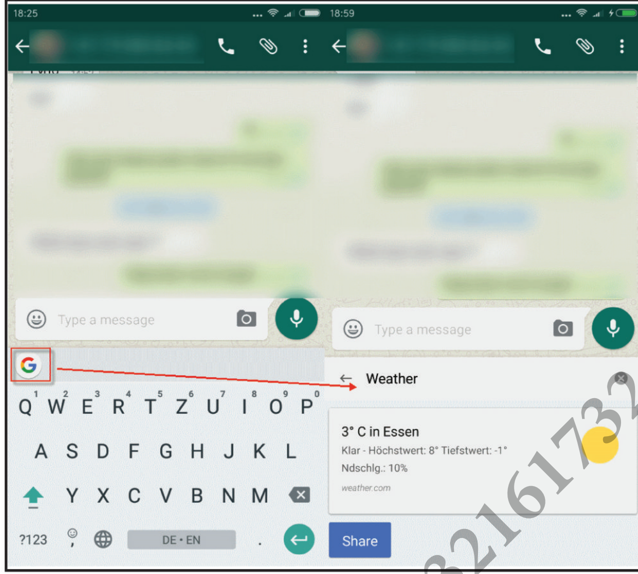
bit.ly/safeeraser



گوگل ''جی بورڈ'' پر موجود ''جی آئی کن'' کیا ہے اور اسے کیسے چھپائیں؟

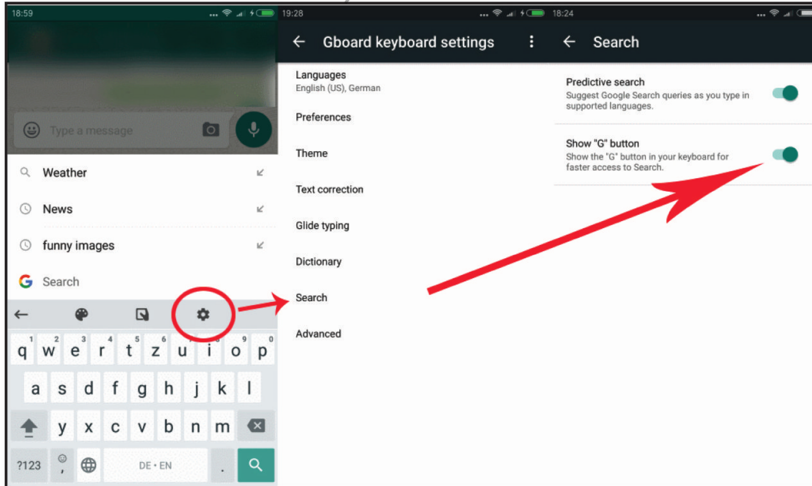
گوگل نے حال ہی میں اینڈرائیڈ میں موجود اپنے کی بورڈ کو اپ ڈیٹ کرتے ہوئے اس میں ایک نیا سرچ کا فیچر بھی فراہم کیا ہے۔ جس کی مدد سے آپ کہیں بھی کچھ لکھنے کے لیے جب کی بورڈ کھولیں تو اوپر ہی گوگل کا آئی کن موجود ہوتا ہے جس کی مدد سے آپ خبریں، موسم کا احوال و دیگر چیزیں تلاش کر کے پیغام میں بھیج سکتے ہیں۔ چاہے آپ ایس ایم ایس کر رہے ہوں یا وٹس ایپ پر کسی سے چیٹ کی بورڈ پر ''جی آئی کن'' موجود ہوتا ہے۔ اس نئی اپ ڈیٹ سے اب گوگل کی بورڈ بھی ''جی بورڈ'' کہلانے لگا ہے۔

اس بٹن کی موجودگی سے چیٹ کرنا انتہائی آسان اور دلچسپ ہو جاتا ہے۔ وہ اس طرح کہ اگر آپ کسی کوئی مزاحیہ تصویر بھیجنا چاہتے ہیں تو ضروری نہیں کہ براؤزر میں گوگل کھولیں اور پھر اسے تلاش کریں، بلکہ جی آئی کن کے ذریعے آپ جو چاہیں یہیں تلاش کرتے ہوئے بھیج سکتے ہیں۔ اس کے علاوہ چونکہ چیٹ کرتے ہوئے ہم اپنے جذبات کا اظہار کرنے کے لیے ایموجیز کا بھی استعمال کرتے ہیں اس لیے یہ بٹن ہر ایموجی کو بھی پہچانتا ہے یعنی اگر آپ ایموجی آئی کن کو منتخب کرتے ہوئے سرچ میں Happy لکھیں گے تو فوراً خوشی والی ایموجی حاضر ہو جائے گی اور آپ اسے دوست کو بھیج سکیں گے۔ یہ سب نئے فیچرز اس ''جی آئی کن'' کی وجہ سے ہیں جس نے گوگل کی بورڈ کو بدل کر ''جی بورڈ'' بنا دیا ہے۔



ویسے تو یہ انتہائی کارآمد فیچر ہے لیکن اکثر لوگ اسے پسند نہیں کرتے اور وہ اسے اپنے کی بورڈ سے فارغ کرنا چاہتے ہیں۔ اگر آپ بھی چاہتے ہیں کہ یہ آئی کن آپ کے کی بورڈ پر نظر نہ آئے تو اسے با آسانی یہاں سے غائب کیا جا سکتا ہے اور پھر کبھی ضرورت پڑنے پر واپس بھی حاصل کیا جا سکتا ہے۔

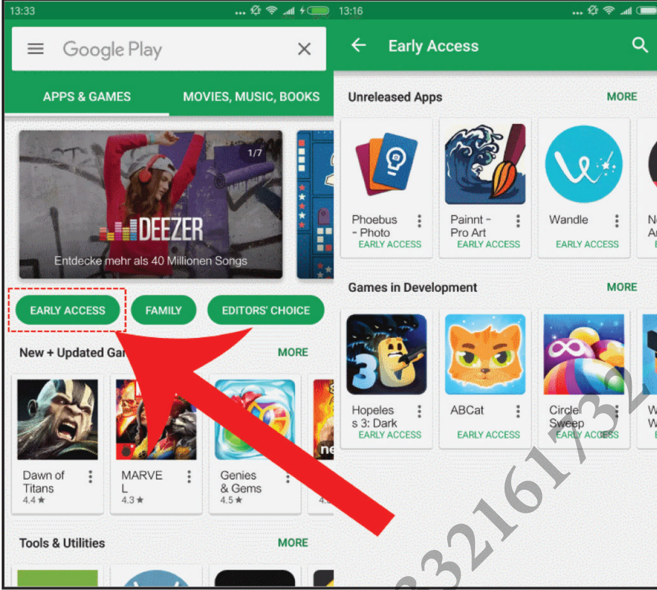
اس کے لیے کہیں کچھ لکھنے کے لیے کی بورڈ کھولیں اور ''جی آئی کن'' پر ٹچ کریں، اس کی سرچ بار کے ساتھ ساتھ اس کے آپشنز آئی کنز بھی ظاہر ہو جائیں گے۔ یہاں موجود گیئر آئی کن جو کہ اس کی سیٹنگز کا مینو ہے کو منتخب کر لیں۔ سیٹنگز جب کھل جائیں تو یہاں ''سرچ'' کے حصے میں آ جائیں۔ یہاں آپ Show "G" Button کے سامنے موجود سلائیڈر کو کھسکاتے ہوئے اسے غیر فعال یعنی آف کر سکتے ہیں۔



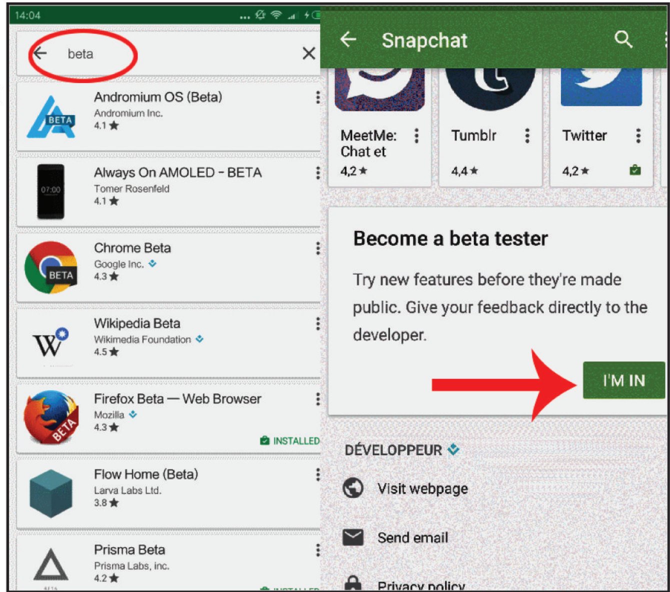
اینڈرائیڈ ایپلی کیشنز ریلیز ہونے سے قبل ہی استعمال کریں

ہر پروگرام و ایپلی کیشن کو جاری کرنے سے پہلے اس کی آزمائش کی جاتی ہے تا کہ فائنل ریلیز سے قبل اس میں موجود خامیوں کو دریافت کر کے دُرست کیا جا سکے۔ اس کام کو آسان بنانے کے لیے ایپلی کیشنز بنانے والے ان کے بی ٹا (Beta) ورژن ریلیز کرتے ہیں تا کہ لوگ انھیں استعمال کر کے ان میں موجود نقائص کی نشاندہی کر سکیں، کیونکہ جب زیادہ لوگ اسے مختلف ڈیوائسز پر استعمال کرتے ہیں تو زیادہ اچھی طرح پروگرام کی کارکردگی کا پتا چلتا ہے۔

گوگل پلے اسٹور پر بھی یہ سہولت دی گئی ہے کہ ڈیولپرز اپنی ایپلی کیشنز کے بی ٹا اور ابھی تک زیرِ تکمیل ورژن کو عوام کے لیے پیش کر سکیں۔ چونکہ ان ایپس میں خرابی ہو سکتی ہے اس لیے گوگل انھیں سبھی کے سامنے پیش نہیں کرتا، آپ کو خصوصی طور پر Beta لکھ کر ان ایپس کو تلاش کرنا پڑتا ہے لیکن بدستور تمام بی ٹا ایپلی کیشنز نظر نہیں آتیں، مثلاً وٹس ایپ کا بی ٹا ورژن بی ٹا پروگرام کو جوائن کیے بغیر نظر نہیں آتا۔



اس لیے ان تک پہنچنے کا سب سے آسان طریقہ تو یہ ہے کہ آپ ''بی ٹا ٹیسٹر'' (Beta Tester) بن جائیں۔ یہ بہت ہی آسان ہے، گوگل پلے اسٹور پر کوئی بھی ایپ جیسے کہ وٹس ایپ یا اسنیپ چیٹ وغیرہ کو کھول کر اسکرول کرتے ہوئے نیچے آتے جائیں جہاں بی ٹی ٹیسٹر بننے کا آپشن موجود ہوگا۔ I am in کے بٹن کے ذریعے آپ بی ٹا ٹیسٹر بن جائیں گے اور اب اگر آپ کسی ایپ کو تلاش کریں گے اور اس کا بی ٹا ورژن دستیاب ہوگا تو آپ اسے انسٹال کر سکیں گے۔ اس کے علاوہ گوگل نے پلے اسٹور میں ایک نیا فیچر "Early Access" کے نام سے پیش کیا ہے، اس آپشن کے ذریعے آپ تکمیل کے مراحل میں موجود ایپس کو دیکھ سکتے ہیں اور انسٹال بھی کر سکتے ہیں۔ تاہم یاد رکھیں کہ ان ایپس میں موجود کوئی خرابی آپ کے اینڈرائیڈ کو نقصان بھی پہنچا سکتی ہے، یہی وجہ ہے کہ انھیں الگ فہرست میں رکھا جاتا ہے تا کہ کوئی انجانے میں انھیں انسٹال نہ کر بیٹھے۔ لیکن اگر تجربات کرنا پسند کرتے ہیں تو ان ایپس کو استعمال کر سکتے ہیں۔



بلاک سم یا بغیر سم کے اپنا وٹس ایپ اکاؤنٹ کیسے ختم کریں؟

ہمارے ہاں تصدیقی مرحلے میں ناکامی کی وجہ سے کئی سمز کو پی ٹی اے کی جانب سے بلاک کیا گیا ہے یا فرض کریں کسی وجہ سے سم بلاک کردی جاتی ہے تو صارفین سوچتے ہیں کہ ان کے وٹس ایپ اکاؤنٹ کا کیا ہوگا؟ جب سم تک ہی رسائی نہ رہے اور صارف اس کے بدلے نئی سم حاصل کرنے کا اہل بھی نہیں تو وٹس ایپ اکاؤنٹ کو کیسے ختم کیا جائے؟ فون چوری ہونے کی صورت میں کم از کم فوری طور پر سم کو بند کروایا جاسکتا ہے اور جلد از جلد نئی سم حاصل کرکے اپنے وٹس ایپ اکاؤنٹ تک رسائی بھی حاصل کی جاسکتی ہے لیکن جیسے کہ ہم نے ذکر کیا کہ اگر سم تک رسائی ہی ممکن نہ ہو تو وٹس ایپ اکاؤنٹ کو کیسے ختم کیا جائے؟

اس حوالے سے وٹس ایپ نے بڑی واضح ہدایات دے رکھی ہیں کہ اگر آپ اپنا وٹس ایپ اکاؤنٹ ختم کرنا چاہتے ہیں تو اس کے لیے آپ بذریعہ ای میل درخواست بھیج سکتے ہیں۔ چونکہ وٹس ایپ اکاؤنٹ میں ای میل ایڈریس بھی موجود ہوتا ہے اس لیے اگر آپ اُسی ای میل ایڈریس سے میل بھیجیں تو آپ کی درخواست کا جائزہ لینے کے بعد وٹس ایپ اکاؤنٹ کو بند کردیا جائے۔ یہ درخواست درج ذیل ای میل ایڈریس پر بھیجی جائے گی:

support@whatsapp.com

ضروری ہے کہ ای میل کے سبجیکٹ میں درج ذیل لکھا ہو:

"Lost/Stolen: Please deactivate my account"

جبکہ ای میل باڈی میں اپنا نمبر انٹرنیشنل کوڈ کے ساتھ لکھ کر بھیج دیں۔

Lost/Stolen: Please deactivate my account

support@whatsapp.com

Lost/Stolen: Please deactivate my account

00923422507857

Georgia

Send Saved

یہاں یہ بات یاد رکھیں کہ اس صورت میں اکاؤنٹ صرف ڈی ایکٹیویٹ ہوگا مکمل ڈیلیٹ نہیں ہوگا۔ آپ کے دوستوں کے پاس وٹس ایپ میں بدستور آپ کا نام موجود رہے گا اور وہ پیغام بھی بھیج سکتے ہیں لیکن پیغامات پہنچیں گے۔ یہ پیغامات 30 دن تک اس صورت میں رہتے ہیں، اگر آپ دوبارہ اکاؤنٹ ایکٹی ویٹ کرلیں تو یہ پیغامات موصول ہوجائیں گے وگرنہ مکمل طور پر ختم ہوجائیں گے۔ اگر اکاؤنٹ کے ڈی ایکٹی ویٹ کرانے کے 30 دن تک اسے دوبارہ ایکٹی ویٹ نہ کیا جائے تو اسے مکمل طور پر ختم کردیا جاتا ہے۔

چیٹ ہسٹری چونکہ فون میں محفوظ ہوتی ہے اس لیے وہ ختم نہیں ہوسکتی اور چونکہ وٹس ایپ اکاؤنٹ بغیر سم کے بھی استعمال کیا جاسکتا ہے اس لیے اپنی گم شدہ سم کے اکاؤنٹ کو بند کرانا مت بھولیں ورنہ پچھتانا بھی پڑسکتا ہے۔



اب بغیر کسی معلومات کے خود کمپیوٹر رپیئرنگ ماہر بنیں

کمپیوٹر میں آئے دن کسی خرابی کا سامنے آنا ایک معمولی سی بات ہے، اگر اس حوالے سے زیادہ معلومات نہ ہو تو کمپیوٹر اکثر رپیئرنگ شاپ پر لے جانا پڑتا ہے۔ آپ کو اسی مصیبت سے بچانے کے لیے ایک کمپیوٹر ماہر نے اپنا سالوں کا تجربہ استعمال کرتے ہوئے ایسا ''آل اِن ون'' پروگرام تیار کیا ہے جو آپ کے کمپیوٹر کے تقریباً سو فیصد مسائل کو ٹھیک کر سکتا ہے۔ اس پروگرام کا نام ''آل اِن ون، سسٹم ریسکیو ٹول کِٹ'' (ALL IN ONE – SYSTEM RESCUE TOOLKIT) ہے۔ اگر اس کے فیچرز کی بات کی جائے تو انھیں ایک صفحے میں بیان کرنا ناممکن ہے۔ یہ ٹول کِٹ دراصل درجنوں ٹولز پر مشتمل ہے جو کمپیوٹر کے تقریباً تمام مسائل کو حل کرنے کی صلاحیت رکھتے ہیں۔

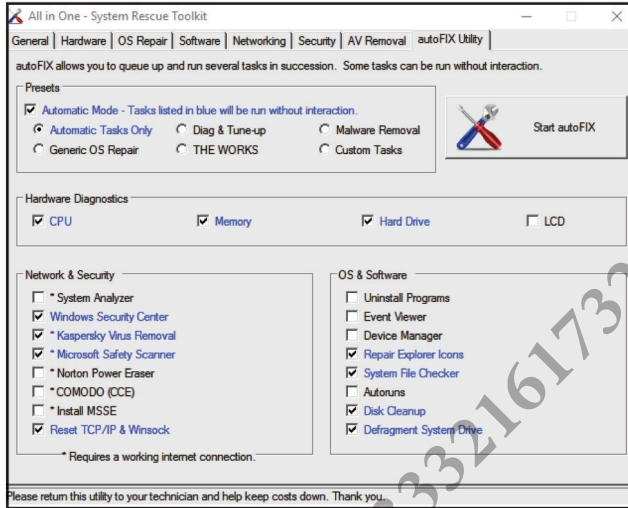
یہ ٹول کِٹ 682 MB سائز کی بوٹ ایبل ڈِسک ہے جسے آپ سی ڈی یا یو ایس بی فلیش ڈرائیو کے ذریعے استعمال کر سکتے ہیں۔

اس کِٹ میں موجود ٹولز سسٹم کے عمومی، ہارڈ ویئر، آپریٹنگ سسٹم، سافٹ ویئر، نیٹ ورکنگ اور سکیوریٹی سمیت تقریباً تمام مسائل کو حل کر سکتے ہیں۔ اکثر اینٹی وائرس بدلنا انتہائی مشکل ثابت ہوتا ہے کیونکہ اینٹی وائرس کو انسٹال کرنے سے اَن انسٹال کرنا مشکل کام ہے، یہی وجہ ہے کہ اس ٹول کِٹ میں تقریباً تمام نامور اینٹی وائرس پروگرامز کو اَن انسٹال کرنے کے ٹولز بھی موجود ہیں۔

یہ مکمل ٹول کِٹ آپ درج ذیل ربط سے ڈاؤن لوڈ کر سکتے ہیں:

paul.is-a-geek.org/aio-srt

اس کے علاوہ حال ہی میں اس پروگرام کو مزید آسان بنانے کے لیے اس کا لائٹ ورژن بھی پیش کیا گیا ہے جس کا سائز صرف 6.84 MB ہے۔ یہ لائٹ



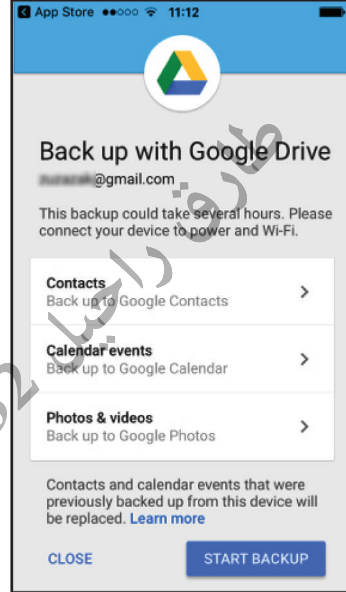
ورژن استعمال میں مزید آسان ہے، اسے ڈاؤن لوڈ کر کے چلائیں تو یہ خود بخود سسٹم کا جائزہ لے کر اس میں موجود خرابیوں کو دُور کرنے کی کوشش کرتا ہے۔ اس کے لیے یہ سسٹم پر سی پی یو کولنگ ٹیسٹ، میموری ٹیسٹ، ہارڈ ڈسک ڈرائیو ٹیسٹ، ونڈوز سکیوریٹی سینٹر چیک، اینٹی وائرس اور اینٹی مال ویئر اسکین، ری سیٹ ونڈوز نیٹ ورکنگ، سسٹم فائل چیکر، ڈسک کلین اپ اور ڈی فریگ چلاتا ہے۔ یعنی یہ ایک ٹول آپ کے سسٹم کو ہر حوالے سے چیک کر کے خود بخود اسے ری اسٹارٹ کرتے ہوئے آپ کے کام کے قابل بنا دیتا ہے۔ اگر آپ کے پاس یہ ٹول موجود ہو تو اس کے بعد آپ کسی کمپیوٹر ماہر کی ضرورت نہیں رہتی۔ یہ لائٹ ورژن درج ذیل ربط سے ڈاؤن لوڈ کریں:

paul.is-a-geek.org/aio-srt/aio-srt-lite



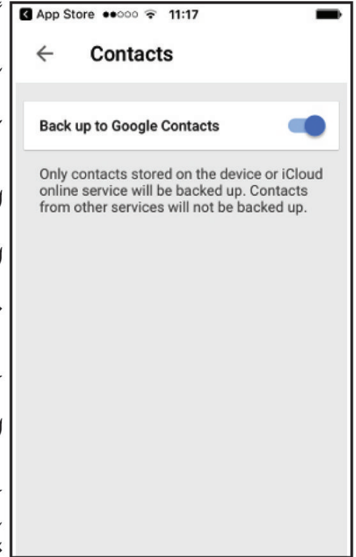
آئی فون سے اپنا تمام ڈیٹا باآسانی اینڈرائیڈ میں منتقل کریں

ایک آپریٹنگ سسٹم سے دوسرے پر منتقل ہونا ہمیشہ ایک مشکل مرحلہ ہوتا ہے۔ جہاں پرانے آپریٹنگ سسٹم کی عادت ہو چکی ہوتی ہیں وہیں اپنا تمام ڈیٹا دوسرے اور نئے آپریٹنگ سسٹم میں منتقل کرنا بھی ایک جھنجٹ محسوس ہوتا ہے۔

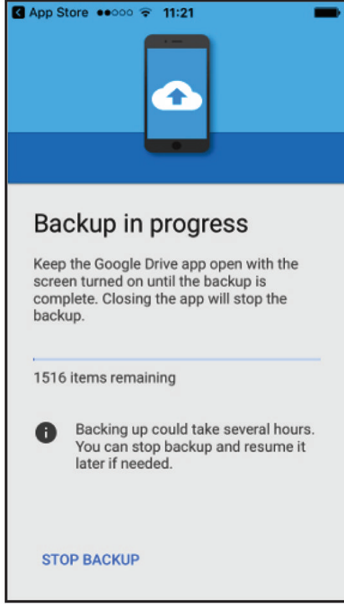


لیکن اگر آپ آئی او ایس سے اینڈرائیڈ پر منتقل ہونا چاہتے ہیں تو یہ کام باآسانی گوگل کے ذریعے کیا جاسکتا ہے۔

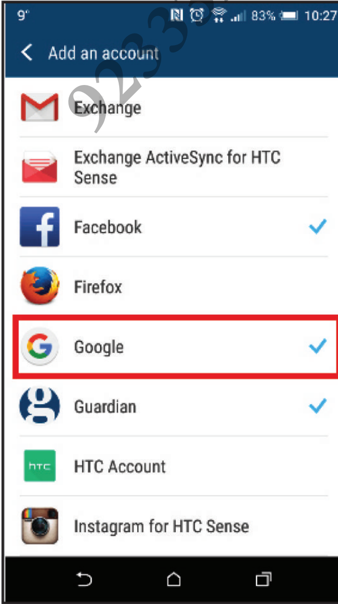
گوگل آپ کو یہ سہولت دیتا ہے کہ اپنا تمام ڈیٹا گوگل ڈرائیو میں بیک اپ کر کے اسے اینڈرائیڈ پر ڈاؤن لوڈ کر لیں۔ یہ عمل خودکار ہوگا اور اس میں آپ کے تمام کونٹیکٹس، تصاویر اور وڈیوز وغیرہ منتقل ہو جائیں گی۔ اس کا دوسرا فائدہ یہ ہے کہ آپ کے اہم ڈیٹا کا بیک اپ بھی بن جائے گا۔



اس کام کو شروع کرنے کے لیے اپنے آئی فون پر گوگل ڈرائیو کا تازہ ترین ورژن انسٹال کرنے کے بعد اس میں اپنا گوگل اکاؤنٹ لاگ اِن کر لیں۔ اس کے بعد اس کی سیٹنگز میں موجود بیک اپ میں آ جائیں۔ اس حصے میں آپ دیکھ سکتے ہیں کون کون سا ڈیٹا گوگل ڈرائیو پر بیک اپ کیا جاسکتا ہے۔ اگر آپ ان میں سے کوئی بیک اپ جیسے کہ کیلنڈر ایونٹس وغیرہ کو بیک اپ نہیں کرنا چاہتے تو اس پر ٹچ کریں اور اگلی کھلنے والی اسکرین پر سلائیڈر کے ذریعے اسے آف کر دیں، یعنی اب اسے بیک اپ نہیں کیا جائے گا۔ اس کے بعد یہاں نیچے موجود



"اسٹارٹ بیک اپ" کے بٹن کو منتخب کریں تو تمام ڈیٹا گوگل ڈرائیو پر بیک اپ ہونا شروع ہو جائے گا۔ آپ کے کانٹیکٹس کو گوگل کانٹیکٹس اور آپ کی میڈیا فائلز کو گوگل فوٹوز پر اپ لوڈ کرنے کا کام شروع ہو جائے گا، آپ کے ڈیٹا کے اعتبار سے اس عمل میں وقت لگ سکتا ہے۔

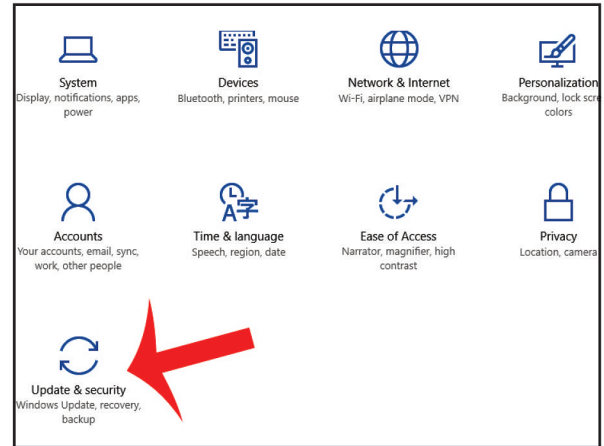


اس کے بعد آپ اینڈرائیڈ پر اپنا گوگل اکاؤنٹ سائن اِن کر کے سیٹنگز میں جا کر اپنا گوگل ڈیٹا سِنک (sync) کر سکتے ہیں، گوگل کے پاس موجود اپنا تمام ڈیٹا آپ فون میں ڈاؤن لوڈ کر سکتے ہیں اور دیکھ بھی سکتے ہیں۔

اب جب چاہیں ونڈوز اپ ڈیٹس کو عارضی طور پر Pause کریں

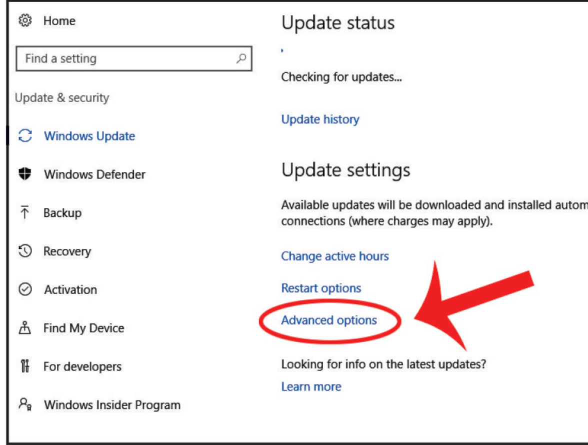
اکثر لوگ ونڈوز کی اپ ڈیٹس سے بہت پریشان رہتے ہیں کیونکہ جب یہ اپ ڈیٹس ڈاؤن لوڈ ہو رہی ہوتی ہیں تو انٹرنیٹ کے ساتھ ساتھ پی سی بھی سست رفتاری کا شکار ہو جاتا ہے۔ اس کے علاوہ کئی اپ ڈیٹس آپریٹنگ سسٹم میں خرابی کا باعث بھی بنتی ہیں مثلاً ونڈوز 10 کی سالگرہ کے موقعے پر خصوصی طور پر جاری ہونے والی اپ ڈیٹس کی وجہ سے کروڑوں صارفین کے ویب کیم نے کام کرنا چھوڑ دیا تھا اور اس کے بعد اگلی آنے والی بڑی اپ ڈیٹس نے صارفین کے انٹرنیٹ کو بند کر دیا تھا۔ ونڈوز صارفین اپ ڈیٹس کو روکنے کے لیے مختلف ترکیبیں استعمال کرتے رہتے ہیں، اکثر تو ونڈوز کی اپ ڈیٹ سروسز کو ہی بند کر دیتے ہیں تاکہ نہ رہے گا بانس اور نہ بجے گی بانسری۔ لیکن زیادہ تر صارفین ایسی باتوں سے لاعلم رہتے ہیں، انھیں پتا ہی نہیں چلتا کہ کب بیک گراؤنڈ میں اپ ڈیٹس ڈاؤن لوڈ ہوئیں، اُنھیں تو تب خبر ہوتی ہے جب یہ انسٹال ہونے کے لیے پی سی کو ری اسٹارٹ کرنے کا تقاضا کر دیتی ہیں۔

اس مسئلے سے نمٹنے کے لیے مائیکروسافٹ نے Pause Update کا فیچر ونڈوز 10 میں فراہم کرنے کا فیصلہ کیا ہے، اس کی بدولت آپ جب چاہیں ونڈوز کی اپ ڈیٹس کو 35 دن تک کے لیے بند کر سکتے ہیں۔ یہ فیچر فی الحال صرف ونڈوز کے تجرباتی ورژنز میں موجود ہے اور عام صارفین تک یہ اپریل

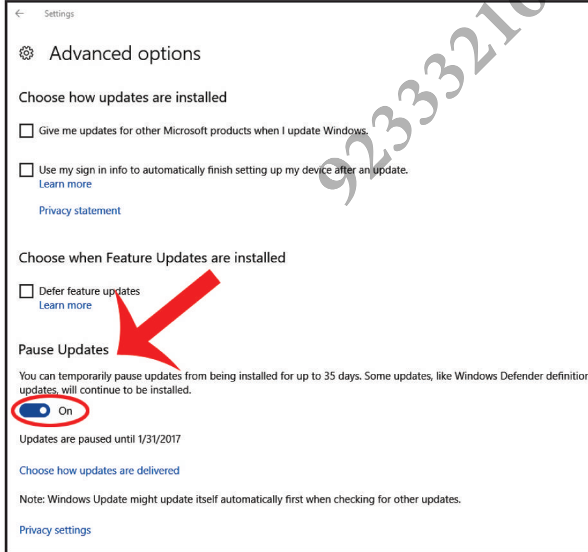


2017 میں پہنچ پائے گا۔

یہ فیچر آپ کے پاس دستیاب ہو جائے تو اسے استعمال کرنے کے لیے



ونڈوز 10 کی سیٹنگز میں سے ''اپ ڈیٹ اینڈ سکیوریٹی'' کے حصے میں آ جائیں۔ یہاں سے ''ایڈوانسڈ آپشنز'' منتخب کریں تو اگلی حصے میں Pause



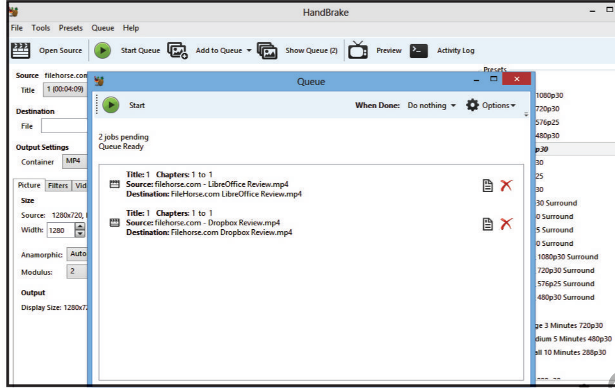
Updates کا آپشن موجود ہوگا۔ یاد رہے کہ اس کے باوجود ونڈوز ڈیفینڈر کی اپ ڈیٹس بدستور فعال رہیں گی تاکہ آپ وائرسز سے محفوظ رہیں۔

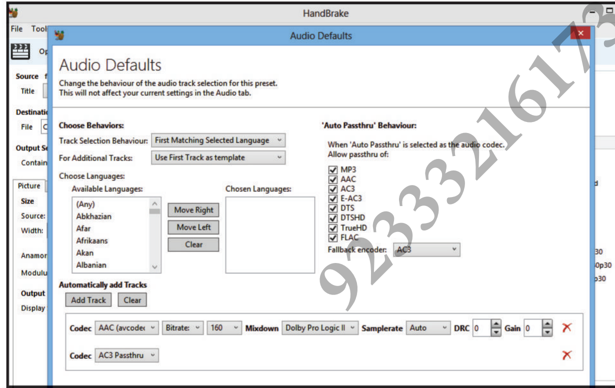
پروفیشنل معیار کا وڈیو کنورٹر مکمل طور پر مفت حاصل کریں

وڈیوز کو کنورٹ کرنا آج سے چند سال قبل اتنا مقبول کام نہیں تھا لیکن آج کل مختلف ڈیوائسز کی آمد کے بعد ہر کسی کو وڈیو کنورٹر کی ضرورت رہتی ہے۔ اکثر تو اسکرین سائز کے لیے وڈیوز کو کنورٹ کرنے کی ضرورت پڑتی ہے مثلاً ڈیسک ٹاپ کے لیے موجود کسی وڈیو کو اسمارٹ فون کے لیے کنورٹ کرنا۔ یا پھر وڈیوز کو شیئر کرنے کے لیے ان کا سائز کم کرنا پڑتا ہے جیسے کہ وٹس ایپ 20 ایم بی سے بڑی وڈیو کو شیئر کرنے کی سہولت نہیں دیتی اس لیے ہمیں وڈیو کا سائز ہی کم کرنا پڑتا ہے۔ یہ بھی ہوسکتا ہے کہ آپ کے پاس کوئی پرانی ڈی وی ڈی یا سی ڈی موجود ہو جسے کمپیوٹر پر دیکھنے کے لیے آپ کنورٹ کرنا چاہتے ہوں۔

ان تمام عوامل میں آپ کے پاس ایک اچھا وڈیو کنورٹر پروگرام موجود ہونا ضروری ہے۔ ایک اچھی خبر یہ ہے کہ گزشتہ 13 سالوں سے ڈیولپمنٹ کے مراحل میں موجود بہترین وڈیو کنورٹر ''ہینڈ بریک'' (HandBrake) کا آخر کار پہلا ورژن ریلیز کر دیا گیا ہے۔ یہ پروگرام انتہائی عمدہ کارکردگی کا حامل ہونے کے باوجود تاحال بی ٹا ورژن تھا اور وہ بھی پچھلے تیرہ سال سے۔ اس کی اپ ڈیٹس مسلسل آ رہی تھیں لیکن اس کے کسی ورژن کو فائنل کا درجہ نہیں دیا گیا۔ لیکن اب گزشتہ سال کے اختتام پر اور نئے سال کی آمد پر آخر کار اس کا پہلا فائنل ورژن ریلیز کر دیا گیا ہے۔

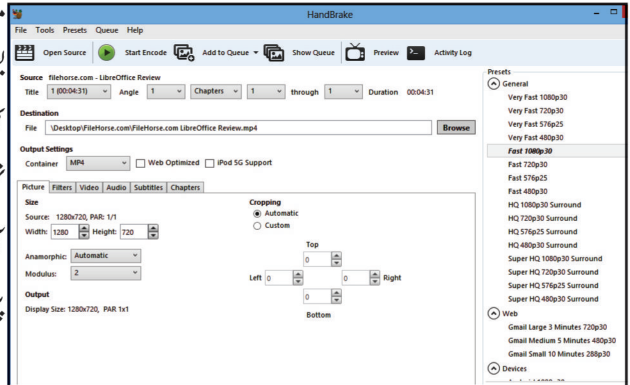
وڈیوز کو کنورٹ کرنے کی بات ہو تو اس کے تمام معروف فارمیٹس کی سپورٹ موجود ہے، آڈیو کے حوالے سے عمدہ کارکردگی موجود ہے اور سب ٹائٹلز شامل کرنے ہوں تو وہ آپشن بھی موجود ہے۔ اس کے علاوہ اس کی سب سے خاص بات یہ ہے کہ یہ پروگرام ونڈوز کے علاوہ لینکس اور میک سسٹم کے لیے بھی بالکل



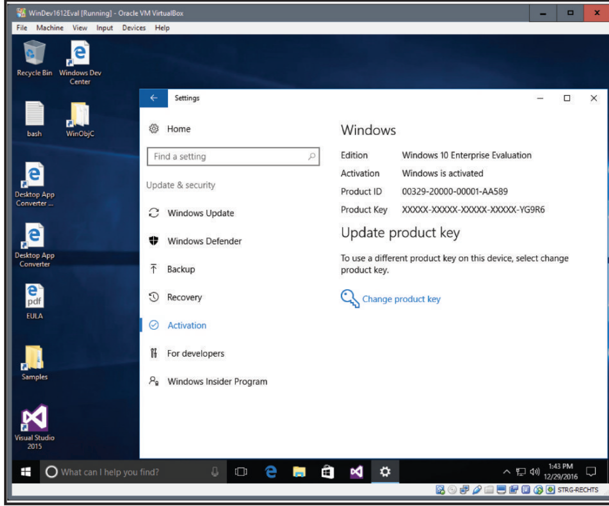


مفت دستیاب ہے بلکہ یہ جی پی یل (GPL) کے لائسنس کے تحت دستیاب ہے یعنی آپ چاہیں تو اس کا سورس کوڈ حاصل کر کے اس میں اپنی من پسند تبدیلیاں بھی خود ہی کر سکتے ہیں۔ اس کے علاوہ اس میں کسی قسم کے کوئی اشتہارات بھی نہیں ہیں۔ اگر آپ ایک پروفیشنل اور مفت وڈیو کنورٹر حاصل کرنا چاہتے ہیں تو آپ کا انتخاب ''ہینڈ بریک وڈیو کنورٹر'' ہی ہونا چاہیے۔ مبتدی حضرات پہلے اس پروگرام کو استعمال کرنے کا طریقہ کار پڑھنا مت بھولیں۔

handbrake.fr



ونڈوز 10 ورچوئل مشین بمع دیگر اہم پروگرامز مفت ڈاؤن لوڈ کریں



مائیکروسافٹ کی اس وقت سب سے بڑی ترجیح UWP یعنی یونی ورسل ونڈوز پلیٹ فارم کا قیام ہے۔ اس پلیٹ فارم کے تحت ایسی اپلی کیشنز بنائی جائیں گی جس میں آپریٹنگ سسٹم نہیں بلکہ ڈیوائس کو مدِنظر رکھا جائے گا۔ چونکہ آج کل مائیکروسافٹ ونڈوز چاہے کمپیوٹر پر موجود ہو یا اسمارٹ فون پر ان کے لیے ایک ہی ایپ اسٹور بنایا گیا ہے اور اس سے ڈاؤن لوڈ کی گئی اپلی کیشنز اسمارٹ فون پر بھی کام کرتی ہیں اور ڈیسک ٹاپ کمپیوٹر پر بھی۔

یہ نظام تبھی فروغ پا سکتا ہے جب زیادہ سے زیادہ افراد مائیکروسافٹ کا تازہ ترین آپریٹنگ سسٹم یعنی ونڈوز 10 استعمال کریں، یہی وجہ ہے کہ مائیکروسافٹ تمام پرانے آپریٹنگ سسٹمز کو تیزی سے نئے آپریٹنگ سسٹم پر اپ گریڈ کرانے میں کوشاں ہے۔

اس حوالے سے مائیکروسافٹ نے ایک تازہ پیش رفت یہ کی ہے کہ اب ونڈوز 10 کی ورچوئل مشینز بھی مفت ڈاؤن لوڈنگ کے لیے فراہم کردی ہیں۔ یہ ورچوئل مشین ونڈوز 10 انٹرپرائز اور پروفیشنل پر مبنی ہیں جب کہ ان میں کئی اضافی اور اہم پروگرامز بھی موجود ہیں۔ دراصل ان ورچوئل مشینز کو فراہم کرنے کا مقصد یہ ہے کہ ڈیولپرز آسانی کے ساتھ یونی ورسل ونڈوز پلیٹ فارم کے تحت اپلی کیشنز بنانے کا کام کرسکیں۔ یہ مشینز ایک محدود مدت کے لیے دستیاب رہیں گی اور اس مدت کے بعد ان کی معیاد ختم ہو جائے گی۔ ان میں موجود پروگرامز بھی وقت کے ساتھ ساتھ بدل سکتے ہیں۔

ایک ورچوئل مشین کا فائل سائز 20 جی بی ہے، جبکہ ونڈوز 10 پروفیشنل پر مبنی ورچوئل مشین کو استعمال کرنے کے لیے ضروری ہے کہ آپ کے پاس مائیکروسافٹ کی لائسنس یافتہ ونڈوز 10 پروفیشنل موجود ہو۔ دراصل یہ ونڈوز کی امیج ہے جسے آپ Virtual Box یا اس جیسے کسی پروگرام میں استعمال کر سکتے ہیں۔ ڈاؤن لوڈ کرنے کے لیے درج ذیل ربط استعمال کریں:

bit.ly/win10virtual

Windows 10 Enterprise (Evaluation - Build 201612) 20 GB download

This VM will expire on 04/08/2017.

VMWare | Hyper-V | VirtualBox | Parallels

This evaluation virtual machine includes:

- Windows 10 Enterprise Evaluation, Version 1607
- Visual Studio 2015 Community Update 3 (Build 14.0.25425.01)
- Windows developer SDK and tools (Build 14393)
- Microsoft Azure SDK for .NET (Build 2.9.6)
- Windows Bridge for iOS (Build 0.2.161107)
- Windows UWP samples (November 2016 Update)
- Windows Bridge for iOS samples
- Bash on Ubuntu on Windows

Windows 10 Professional (Licensed - Build 201612) 20 GB download

This VM install requires a Windows 10 Pro license (EN-US only).

VMWare | Hyper-V | VirtualBox | Parallels

This licensed virtual machine includes:

- Windows 10 Pro, Version 1607
- Visual Studio 2015 Community Update 3 (Build 14.0.25425.01)
- Windows developer SDK and tools (Build 14393)
- Microsoft Azure SDK for .NET (Build 2.9.6)
- Windows Bridge for iOS (Build 0.2.161107)
- Windows UWP samples (November 2016 Update)
- Windows Bridge for iOS samples
- Bash on Ubuntu on Windows

The Microsoft Software License Terms for the Windows 10 VMs supersede any conflicting Windows license terms included in the VMs.

اینڈرائیڈ پر بیرونی ایپلی کیشنز کو خودکار طریقے سے اپ گریڈ کریں

اینڈرائیڈ کی مقبولیت کی وجہ سے اس کی ایپلی کیشنز انتہائی تیزی سے بنائی جا رہی ہیں۔ اینڈرائیڈ ایپس ویسے تو گوگل پلے اسٹور سے انسٹال کی جاتی ہیں لیکن اکثر ایپلی کیشنز جب کسی وجہ سے پلے اسٹور سے انسٹال نہ ہو سکیں تو اینڈرائیڈ صارفین انھیں کہیں اور سے ڈاؤن لوڈ کر کے انسٹال کر لیتے ہیں۔ پلے اسٹور کے ذریعے سے انسٹال ہونے والی تمام ایپلی کیشنز کے جب نئے ورژن اسٹور پر دستیاب ہوتے ہیں تو اینڈرائیڈ انھیں خود بخود اپ گریڈ کر دیتا ہے۔ لیکن ایسی ایپس جنھیں گوگل پلے اسٹور سے انسٹال نہ کیا ہو، انھیں اپ ڈیٹ کرنے کے لیے ضروری ہوتا ہے کہ دوبارہ ان کا تازہ ورژن ڈاؤن لوڈ کر کے انسٹال کیا جائے۔

ایسی درجنوں ایپس آج کل تقریباً ہر اینڈرائیڈ صارف کے اسمارٹ فون میں موجود رہتی ہیں اور ان کا اپ ڈیٹ نہ ہونا کئی مسائل کو جنم دیتا ہے۔ اکثر تو یہ کام کرنا ہی چھوڑ دیتی ہیں اور دوسرا ان کا پرانے ورژن پر موجود رہنا بھی ایک سکیورٹی خطرہ ہے کہ ان میں دریافت ہونے والی خرابی چونکہ نئے ورژن میں ٹھیک کی گئی ہوتی ہے لیکن نئے ورژن کی عدم انسٹالیشن کی وجہ سے فون خطرے میں رہتا ہے۔

ایسی صورتِ حال میں آپ کے پاس ''اے پی کے اپ ڈیٹر'' (APKUpdater) ایپلی کیشن انسٹال ہونی چاہیے۔ یہ ایپلی کیشن ایسی بیرونی انسٹال ایپلی کیشنز پر نظر رکھتی ہے اور جیسے ہی ان کا تازہ ترین ورژن دستیاب ہوتا ہے انھیں اپ گریڈ کر سکتی ہے۔

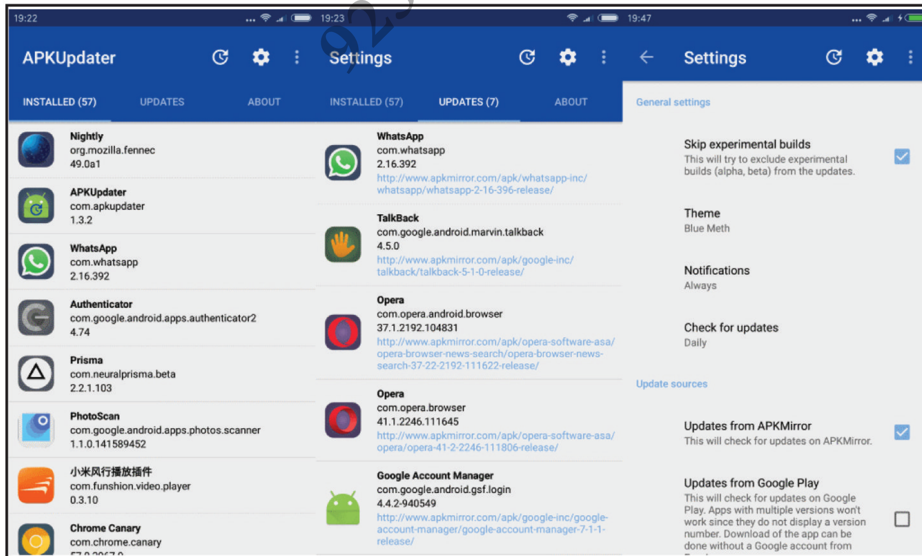
یہ ایپلی کیشن بھی بطور APK فائل دستیاب ہے جسے آپ درج ذیل ربط سے ڈاؤن لوڈ کر کے اپنے فون میں انسٹال کر سکتے ہیں:

bit.ly/apkupdater

یہ ایپ app-release.apk کے نام سے موجود ہوگی اور اس کا تازہ ترین ورژن مفت ڈاؤن لوڈ کیا جا سکتا ہے۔ انسٹالیشن کے بعد جب آپ اسے چلائیں گے تو یہ انسٹال شدہ تمام ایپس کی فہرست سامنے پیش کر دے گی۔ اگر آپ کسی ایپلی کیشن کو اپ ڈیٹ کرنے میں دلچسپی نہیں رکھتے تو یہ آپشن بھی اس ایپ میں موجود ہے۔ اس کے علاوہ اگر آپ ایپلی کیشن کے تکمیلی ورژن یعنی بی ٹا ورژن سے بچنا چاہتے ہیں تو ایپ کنفیگریشن میں جا کر "Skip experimental builds" کے آپشن کو استعمال کریں۔

''اے پی کے اپ ڈیٹر'' ایپلی کیشنز کو اپ ڈیٹ کرنے کے لیے APKMirror ویب سائٹ کو استعمال کرتی ہے جبکہ گوگل پلے اسٹور اور APKPure کو بھی اس فہرست میں شامل کیا جا سکتا ہے۔

اس طرح وہ بیرونی ایپلی کیشنز جو پہلے مہینوں پرانے ورژن پر موجود ہوں گی اُن کو آپ اس ایپ کے ذریعے جب چاہیں اپ گریڈ کر سکتے ہیں۔



اب گرافکس کارڈ کے بغیر اپنے عام پی سی پر جدید ترین گیمز کھیلیں

اگر آپ گیمز کھیلتے ہیں تو یقیناً جانتے ہوں گے کہ گیمز کا ہر نیا آنے والے ورژن کس قدر زیادہ ہارڈویئر کا متقاضی ہوتا ہے۔ صرف دو سے تین سال پرانا کمپیوٹر آج کے نئے گیم کو چلانے سے قاصر ہوتا ہے۔ اس لیے اگر آپ گیم کا نیا سے نیا ورژن کھیلنا چاہتے ہیں تو یہ انتہائی ضروری ہوجاتا ہے کہ ہارڈ ویئر کو بھی اپ گریڈ کرتے رہیں۔ وہ لوگ جن کے کمپیوٹر میں مزید ہارڈ ویئر نصب کرنے کی گنجائش نہیں ہوتی خاص کر لیپ ٹاپ صارفین وہ ایسی صورتِ حال میں صرف صبر ہی کر سکتے ہیں کہ وہ چاہتے ہوئے بھی گیمز کے تازہ ورژن کا لطف نہیں اُٹھا سکتے اور اگر ان کے لیپ ٹاپ میں تھری کارڈ موجود نہ ہو تو پھر تو سمجھیں وہ کوئی بھی اچھا گیم نہیں کھیل سکتے۔

تھری ڈی گرافکس کارڈ کے حوالے سے ''این ویڈیا'' (Nvidia) کا نام کسی تعارف کا محتاج نہیں، اس کمپنی کے بنائے ہوئے گرافکس کارڈ گیمز کھیلنے کے لیے سب سے بہترین تصور کیے جاتے ہیں۔ سبھی کی کوشش ہوتی ہے کہ اس کمپنی کا بہترین گرافکس کارڈ ان کے کمپیوٹر میں نصب ہو لیکن ان کی قیمتیں برداشت کرنا سبھی کے بس کی بات نہیں۔ اس معاملے سے نمٹنے کے لیے این ویڈیا نے ایک نئی کاوش ''جی فورس ناؤ'' (GeForce Now) کے نام سے پیش کی ہے۔ جی فورس ناؤ ایک کلاؤڈ گیمنگ سروس ہے، جس میں تازہ ترین اور معروف پچاس گیمز موجود ہیں، ان کو کھیلنے کے لیے صارف کو کسی خاص ہارڈ ویئر کی ضرورت نہیں۔ اسے آپ آن لائن گیمز کہہ سکتے ہیں جن کو کھیلنے کے لیے ہارڈ ویئر این ویڈیا خود فراہم کرے گی نہ کہ یہ آپ کے سسٹم پر اثر ڈالیں گے۔ ان گیمز کو کھیلنے کے لیے ہارڈ ویئر کی ضرورت نہ سہی لیکن تیز ترین انٹرنیٹ کی ضرورت ہے۔ ظاہر ہے اتنے بڑے گیمز کو زبردست گرافکس کے ساتھ آپ کے پی سی یا ٹیبلٹ میں منتقل کرنے کے لیے انٹرنیٹ ہی استعمال ہوگا اس لیے آپ کے پاس کم از کم 10 Mbps کا انٹرنیٹ کنکشن موجود ہونا چاہیے۔ اگر آپ 1080p 60FPS گیمز کا انتخاب کرتے ہیں تو انٹرنیٹ کنکشن بھی 50Mbps کی رفتار کا حامل ہونا چاہیے۔ اس کے علاوہ آپ کو درج ذیل اشیا کی ضرورت ہوگی:

این ویڈیا شیلڈ کنٹرولر یا گیم پیڈ

5GHz بینڈ اور این ویڈیا شیلڈ کی سپورٹ کا حامل وائی فائی راؤٹر

این ویڈیا ڈیوائس جیسے کہ این ویڈیا اینڈرائیڈ ٹی وی، این ویڈیا شیلڈ پورٹ ایبل یا این ویڈیا شیلڈ ٹیبلٹ

اس کے بعد این ویڈیا کی ویب سائٹ سے گیمز کھیلنے کی سبسکرپشن حاصل کی جا سکتی ہے جو کہ 7.99 امریکی ڈالر ماہانہ ہے جبکہ پہلا مہینہ مفت۔ اس سروس کو عمدہ طریقے سے فراہم کرنے کے لیے این ویڈیا نے دنیا کے ممتاز ممالک میں اپنے ڈیٹا سرورز نصب کیے ہیں تاہم یہ سروس فی الحال صرف امریکا، کینیڈا، یورپ اور جاپان میں دستیاب ہے۔ مزید تفصیلات کے لیے یہ ربط ملاحظہ کیجیے:

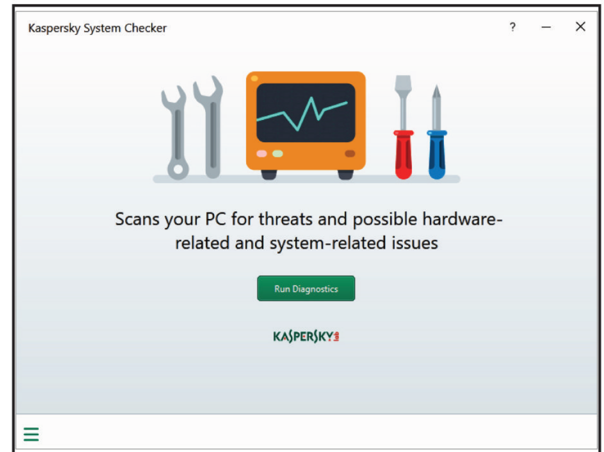
bit.ly/geforcenow

سافٹ ویئر، ہارڈ ویئر اور وائرس کے مسائل پر با آسانی قابو پائیں

کمپیوٹرز کے ساتھ آئے دن نت نئے مسائل پیش آتے رہتے ہیں۔ ان نئے نئے مسئلوں سے نمٹنے سبھی کے بس کی بات نہیں ہوتی۔ خاص طور پر جو لوگ کمپیوٹر کے حوالے سے زیادہ معلومات نہیں رکھتے وہ تو یہ فرق بھی نہیں کر پاتے کہ مسئلہ ہارڈ ویئر کا ہے یا سافٹ ویئر کا، کوئی وائرس زدہ پروگرام انسٹال ہو گیا ہے یا سسٹم پر وائرس نے حملہ کر دیا ہے۔ ان باتوں کو سمجھنا سبھی کے لیے آسان نہیں ہوتا۔ اسی لیے معروف کمپیوٹر سیکیورٹی کمپنی ''کیسپر سکی'' نے ایک نیا پروگرام ''سسٹم چیکر'' کے نام سے پیش کیا ہے۔

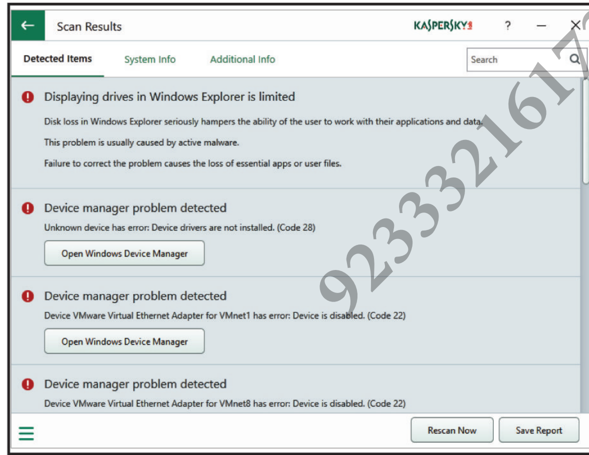
یہ پروگرام اینٹی وائرس بھی ہے اور سسٹم کے دیگر مسائل کو بھی تلاش کر سکتا ہے چاہے وہ سافٹ ویئر کے حوالے سے ہوں یا ہارڈ ویئر کے حوالے سے۔ اس کی سب سے اچھی بات اس کا پورٹ ایبل ہونا ہے۔ یعنی اسے استعمال کرنے کے لیے ضروری نہیں کہ آپ اسے انسٹال کریں۔ بس ضرورت پڑنے پر آپ اسے ڈاؤن لوڈ کر کے چلا سکتے ہیں۔

یہ ٹول چند منٹس میں ہی مکمل سسٹم کو اسکین کر سکتا ہے لیکن اگر آپ نے درجنوں پروگرامز انسٹال کر رکھے ہیں اور آپ کے پی سی میں بہت زیادہ ڈیٹا موجود ہے تو یہ اسکیننگ کچھ طویل بھی ہو سکتی ہے۔ لیکن اگر آپ اسے اسکیننگ مکمل کرنے دیں تو اس کے نتائج آپ کے کمپیوٹر کے مسائل کو حل کر سکتے ہیں۔



اسکیننگ کے دوران آپ جب چاہیں جتنا کام ہو چکا ہو اس کی رپورٹ ملاحظہ کر سکتے ہیں اور اسکیننگ کو روک بھی سکتے ہیں۔ اسکیننگ کے مکمل ہونے کے بعد آپ کو واضح رپورٹ فراہم کی جائے گی کہ دراصل آپ کے سسٹم میں کیا مسئلہ ہے۔ اگر کوئی وائرس ہو یہ ٹول اسے با آسانی تلاش کر سکتا ہے۔ اگر آپ کے سسٹم پر پہلے سے ہی اینٹی وائرس انسٹال ہے تب بھی یہ ٹول کام کر سکتا ہے اور آپ کے اینٹی وائرس کو چھیڑے بغیر پورا سسٹم اسکین کر سکتا ہے۔

جیسا کہ ہم نے ذکر کیا کہ یہ وائرس کے علاوہ ونڈوز کے دیگر مسائل کو بھی ڈھونڈ سکتا ہے مثلاً اگر آپ کے پاس ونڈوز کی کسی غلط کنفگریشن کی وجہ سے کوئی مسئلہ آ رہا ہے تو یہ آپ کی توجہ اس جانب دلا سکتا ہے۔ یہی نہیں اگر سسٹم میں موجود کوئی ہارڈ ویئر درست طریقے سے اپنا کام انجام نہیں دے رہا تو اس کے ذریعے آپ یہ بھی جان سکتے ہیں۔ اگر آپ نے غلطی سے کوئی غیر ضروری پروگرام انسٹال کر لیا ہے تو یہ پروگرام اس کی نشاندہی بھی کر سکتا ہے تاکہ آپ اسے اَن انسٹال کر کے سسٹم کو واپس اچھی حالت میں لا سکیں۔ اگر آپ کمپیوٹر کے ہر طرح کے مسائل سے خود ہی نمٹنا چاہتے ہیں تو آپ کے پاس یہ ٹول ضرور موجود ہونا چاہیے، جسے آپ درج ذیل ربط سے مفت حاصل کر سکتے ہیں:



kaspersky.com/system-checker

نئے اور بہترین فیچرز سے لیس اوپرا کا نیا شاہکار براؤزر

اوپرا براؤزر کا نام آپ کو ابھی بھولا نہیں ہوگا۔ اوپرا اپنے دور کا ایک بہترین براؤزر ہے۔ لیکن کافی عرصے سے اس کا استعمال کم ہوتے ہوتے تقریباً ختم ہی ہو چکا ہے سوائے اسمارٹ فونز کے۔ ''اوپرا سافٹ ویئر'' نے دنیا کا جدید اور تیز ترین براؤزر پیش کرنے کا اعلان کیا ہے۔ یہ براؤزر اپنے فیچرز اور شکل کے اعتبار سے دیگر تمام براؤزرز سے نہ صرف یکسر مختلف ہے بالکل اس کی رفتار اور انداز بھی دیگر سب براؤزرز سے جدا ہے۔ یہ براؤزر ابھی صرف آزمائشی بنیادوں پر ڈیویلپر حضرات کے لیے پیش کیا گیا ہے۔

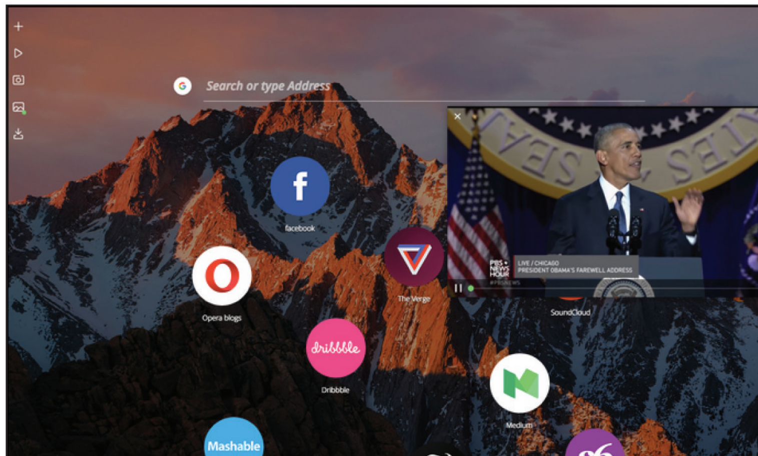


اس نئے براؤزر کو ''نیون'' (Neon) کا نام دیا گیا ہے۔ جیسا کہ ہم نے کہا یہ ابھی تکمیل کے مراحل میں ہے اس لیے فی الحال اس کا صرف تصوراتی ورژن پیش کیا گیا ہے۔ اوپرا نیون کو پیش کرنے والی ٹیم کا کہنا ہے یہ ایک ایسا براؤزر ہوگا جو نہ صرف تیز ترین ہوگا، ہلکا پھلکا ہوگا، سسٹم پر بوجھ نہیں ڈالے اور اپنے فیچرز کی بدولت صارفین کے دل جیت لے گا کیونکہ اسے صرف اور صرف صارفین کے لیے بنایا گیا ہے۔ اس کے پیچھے کمپنی کا کوئی مفاد نہیں۔ صاف ستھرے اور خوبصورت ڈیزائن کا یہ براؤزر واقعی آپ کو پسند آئے گا۔

اس کے انٹرفیس کی بات کی جائے تو اس میں عام براؤزرز کی طرح اوپر کی جانب کوئی ایڈریس بار موجود نہیں جبکہ یہ صارف کی ڈیسک ٹاپ پر موجود تصویر کو ہی اپنے بیک گراؤنڈ کے لیے استعمال کرتا ہے۔ اس میں اہم چیز میڈیا پلیئر کا موجود ہونا ہے جس کے ذریعے آپ یوٹیوب یا کسی بھی ویب سائٹ پر وڈیو کو دیکھتے ہوئے اسے براؤزر ونڈو سے الگ کر سکتے ہیں۔ اس طرح کسی دوسری ویب سائٹ پر کوئی تحریر پڑھتے ہوئے آپ کو دو ونڈوز کو چھوٹا کر کے استعمال نہیں کرنا پڑے گا بلکہ وڈیو اس کے میڈیا پلیئر میں الگ ونڈو میں چلنا شروع ہوجائے گی۔

اس کے علاوہ اکثر لوگ براؤزر میں اسکرین شاٹس لینا پسند کرتے ہیں اس لیے یہ فیچر کسی اضافی ایڈ اون کی مدد سے نہیں حاصل کرنا پڑے گا بلکہ یہ پہلے سے اس براؤزر میں موجود گا اور تمام بنائے گئے اسکرین شاٹس کو منظم رکھنے کے لیے ایک گیلری بھی فراہم کی جائے گی۔

opera.com/computer/neon



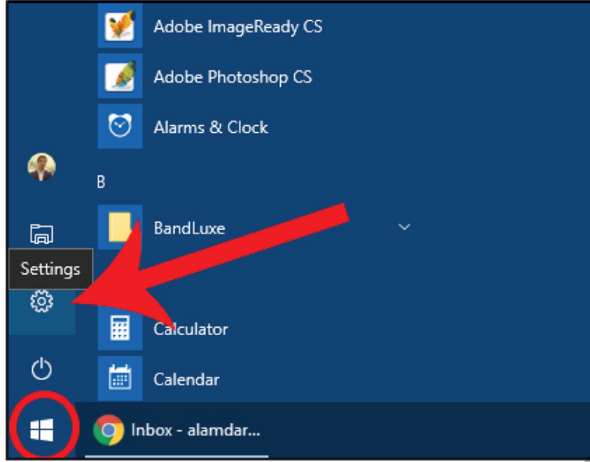
اب ونڈوز 10 کو اپنے چہرے سے لاگ اِن کریں

ونڈوز کو پاس ورڈ کے ذریعے لاگ اِن کرنا ایک عام سی بات ہے۔ ونڈوز 10 میں مائیکروسافٹ نے اس طریقے کو جدید بناتے ہوئے لاگ اِن ہونے کے کئی طریقے فراہم کیے ہیں۔ مثلاً پن، فنگر پرنٹس اور چہرے کی شناخت سے۔ اگر آپ کے سسٹم میں فنگر پرنٹ ریڈر موجود ہے تو ونڈوز 10 میں اسے استعمال کیا جاسکتا ہے۔ اس کے علاوہ ونڈوز 10 کا نیا اور بہترین فیچر ''ونڈوز ہیلو'' ہے جس کی مدد سے چہرے کی شناخت کرانے کے بعد ونڈوز کو خودکار طریقے سے لاگ اِن کیا جاسکتا ہے۔ پاس ورڈ کو بھولنا ایک عام سی بات ہے لیکن چہرے کو یاد رکھنا جب کمپیوٹر کی ذمے داری ہو تو صارف بے فکر ہو جاتا ہے۔

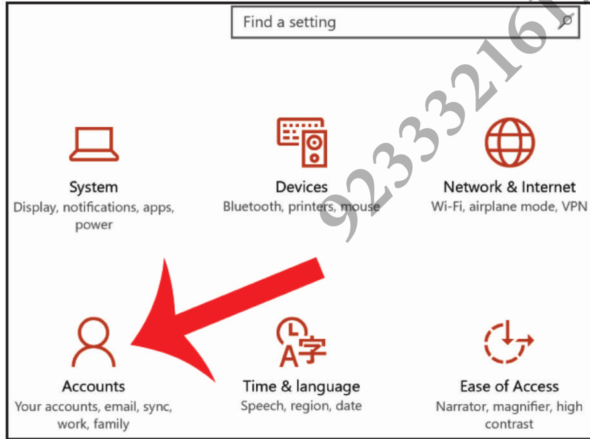
یہ اُس صورت میں بھی بہترین ہے جب ایک ہی کمپیوٹر کو کئی لوگ استعمال کرتے ہوں اور سب بار بار شکایت کریں کہ وہ پاس ورڈ بھول چکے ہیں، چہرے کی شناخت سے سب با آسانی اپنے اپنے اکاؤنٹ میں لاگ اِن ہو سکتے ہیں۔ اس کے علاوہ اگر آپ کئی لوگوں کے کمپیوٹرز کا نظام سنبھالتے ہیں اُس صورت میں اس آپشن کو استعمال کریں تو سب آپ کو پاس ورڈ ری سیٹ کرنے کے لیے تنگ نہیں کریں گے۔ یہ فیچر انتہائی برق رفتاری سے کام کرتا ہے اور جب لاگ اِن اسکرین کے سامنے اس کے پاس محفوظ شدہ چہرہ موجود ہو تو یہ اُسے پہچانتے ہی فوراً کمپیوٹر لاگ اِن کر سکتا ہے۔

آئیے آپ کو بتاتے ہیں کہ کس طرح ونڈوز 10 میں ''ونڈوز ہیلو'' کو فعال کرنا بہت ہی آسان ہے بس آپ کے کمپیوٹر میں اس کی سپورٹ موجود ہونی چاہیے، اگر آپ کا کمپیوٹر اس خاصیت کا حامل نہیں تو یہ فیچر آپ استعمال نہیں کر سکیں گے۔



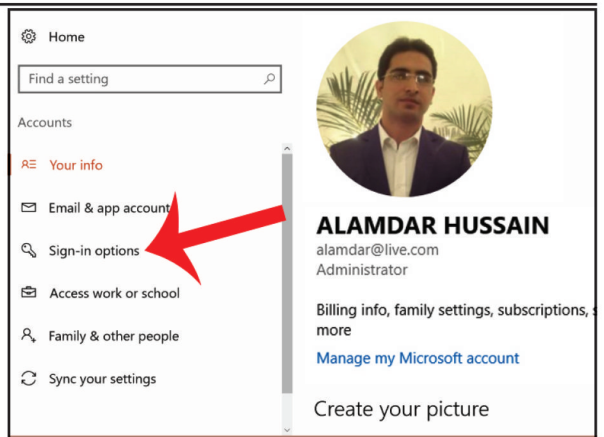


سب سے پہلے ونڈوز اسٹارٹ مینو پر کلک کرتے ہوئے ''سیٹنگز'' کھول لیں۔



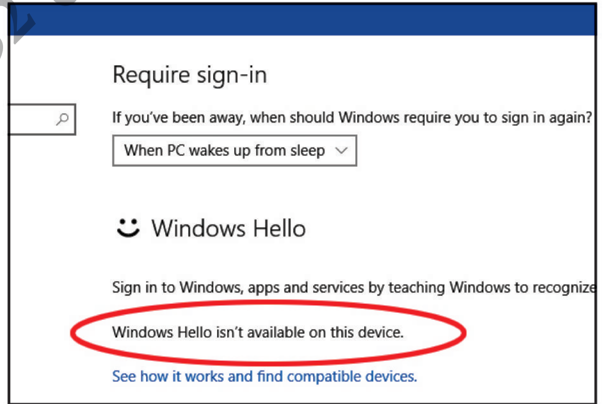
سیٹنگز کھل جائیں تو یہاں موجود ''اکاؤنٹس'' کے حصے میں آجائیں۔

اب اگلی اسکرین پر سے آپ کو ''سائن اِن آپشنز'' کو منتخب کرنا ہے۔ اسی حصے میں آپ ونڈوز ہیلو کو سیٹ اپ کر سکتے ہیں اور یہ بھی جان سکتے ہیں کہ آپ کی ڈیوائس میں اس کی اہلیت موجود ہے یا نہیں۔ اور وہ کون کون سی ڈیوائسز ہیں جن میں اس فیچر کو استعمال کیا جا سکتا ہے۔ زیادہ تر یہ فیچر آپ اچھی ڈیوائسز میں

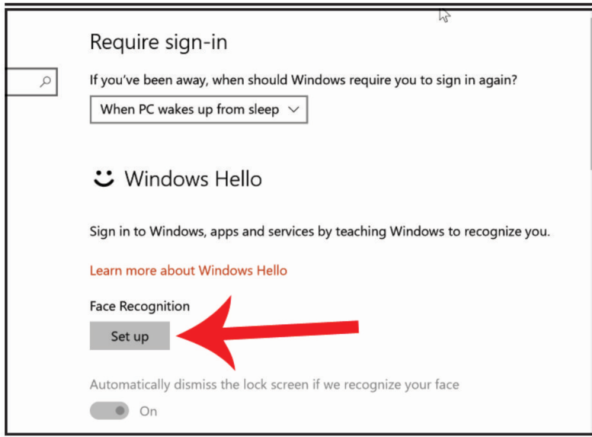


استعمال کر سکتے ہیں کیونکہ اسے استعمال کرنے کے لیے ویب کیم کا ہونا بہت ضروری ہے۔ ویب کیم کو استعمال ہوئے ہی ونڈوز صارف کو پہچانتی ہے، تاہم صرف ویب کیم کی موجودگی ہی کافی نہیں، جیسے کہ ہم نے پہلے بھی ذکر کیا ہے کہ یہ فیچر صرف اچھے اور بہترین لیپ ٹاپس، اسمارٹ فون اور ونڈوز سرفیس ٹیبلٹس میں استعمال کیا جاسکتا ہے۔ اگر آپ کو یہاں یہ لکھا نظر آئے کہ:

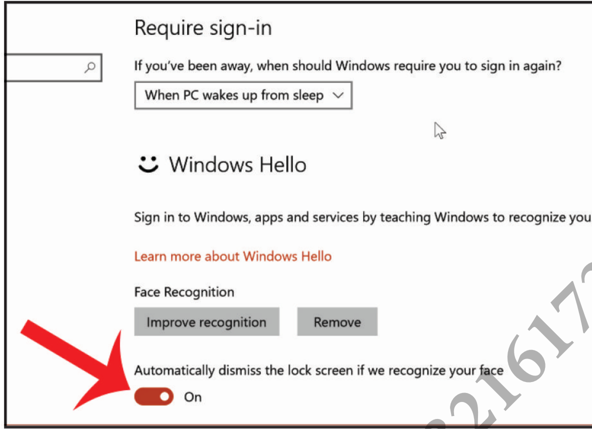
Windows Hello isn't available on this device.



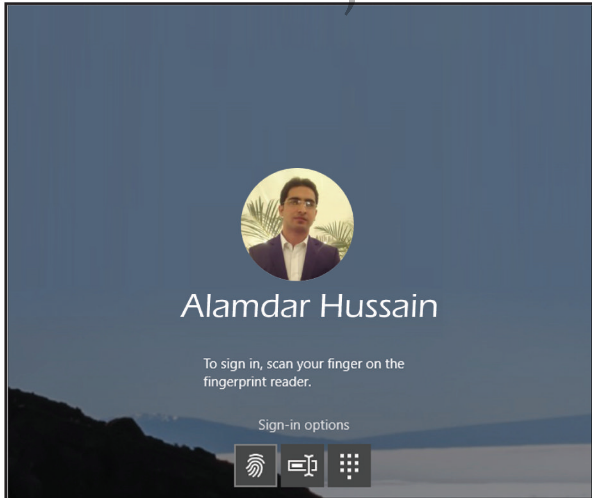
تو اس کا مطلب ہے کہ آپ کی ڈیوائس میں اس فیچر کو استعمال کرنے کی اہلیت موجود نہیں وگرنہ یہاں آپ کو ''سیٹ اپ'' کا بٹن ملے گا جسے استعمال کرتے ہوئے اس فیچر کو فعال کیا جاسکتا ہے۔ سیٹ اپ پر کلک کرنے سے آپ کو ''ونڈوز ہیلو'' میں خوش آمدید کہا جائے گا، جبکہ اگلے مرحلے پر ویب کیم آپ کے چہرے کو محفوظ کرنے کا کام شروع کردے گا۔ اس کے لیے آپ کو چند سیکنڈز تک ویم کیم کی جانب دیکھتے رہنا ہوگا۔ یہ کام مکمل ہوتے ہی آپ کو آگاہ کردیا جائے گا کہ اب آپ اس آپشن کو استعمال کرسکتے ہیں۔



اب آپ یہاں سے یہ آپشن بھی فعال کرسکتے ہیں کہ اگر یہ چہرہ ڈیوائس کے سامنے موجود ہو تو ونڈوز اسے پہچانتے ہوئے فوراً لاگ اِن کردے۔

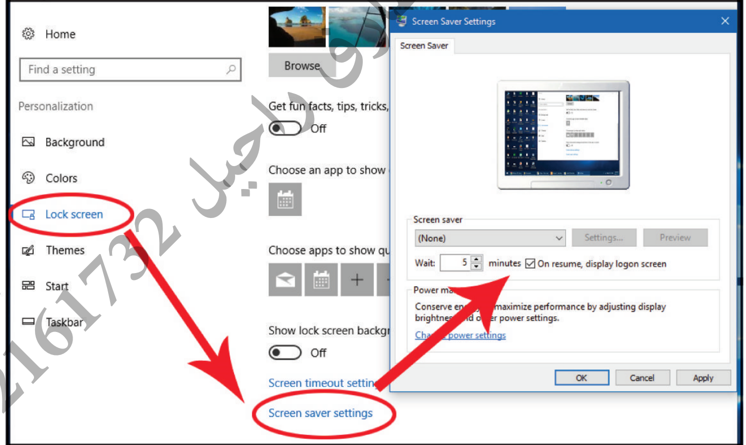


اسی طرح آپ فنگر پرنٹس کے ذریعے لاگ اِن ہونے کی سیٹنگز بھی انجام دے سکتے ہیں۔



اب آپ کا کمپیوٹر اجازت بغیر کوئی استعمال نہیں کر پائے گا

ونڈوز پی سی کو لاک کرنا ایک عام سی عادت ہے۔ جب ہم کمپیوٹر کو آن رکھتے ہوئے کچھ دیر کے لیے کہیں جانا چاہتے ہیں تو اسے لاک کر دیتے ہیں۔ زیادہ تر لوگ اس کے لیے Windows+L کی کمانڈ استعمال کرتے ہیں۔ ان بٹنز کو ایک ساتھ دبانے سے ونڈوز لاک ہوجاتی ہے اور پھر دوبارہ پاس ورڈ کے ذریعے اسے کھولا جاتا ہے۔ اس طرح پی سی دوسروں کی غیر ضروری چھیڑ چھاڑ سے محفوظ رہتا ہے اور آن بھی رہتا ہے تاکہ آپ بروقت دوبارہ کام کا آغاز کر سکیں۔

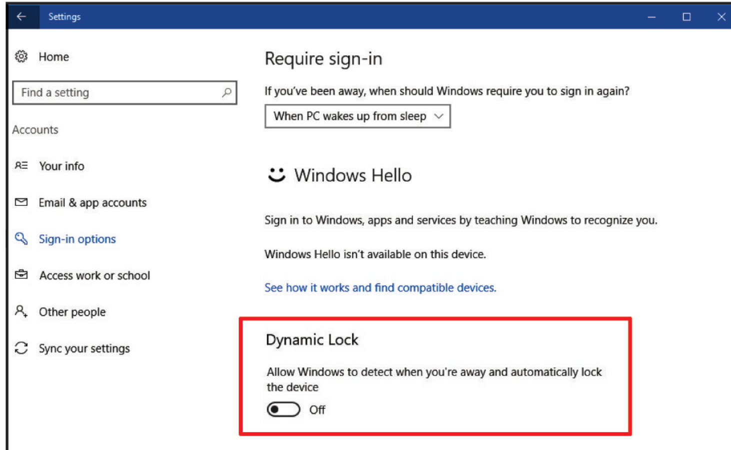


فرض کریں کبھی اگر آپ ونڈوز کو لاک کرنا بھول جائیں، یا آپ چند سیکنڈز کے لیے کہیں جائیں اور یہ دورانیہ طویل ہوجائے تو پریشانی ہوجاتی ہے کیونکہ آپ کا کمپیوٹر جس میں آپ کا اہم اور حساس ڈیٹا موجود ہے کسی کی بھی دسترس میں رہتا ہے۔ ونڈوز پر خودکار لاک کو فعال کر کے اس مسئلے پر قابو پایا جاسکتا ہے۔ اس طرح جب ایک مخصوص دورانیے تک ونڈوز استعمال نہیں ہوگی تو وہ خود بخود لاک ہو جائے گی۔

یہ آپشن ''اسکرین سیور سیٹنگز'' کے اندر موجود ہوتا ہے۔ ونڈوز 10 میں یہ آپشن آپ کو مین سیٹنگز کے اندر ''پرسنلائزیشن'' اور پھر لاک اسکرین کے اندر ملے گا۔

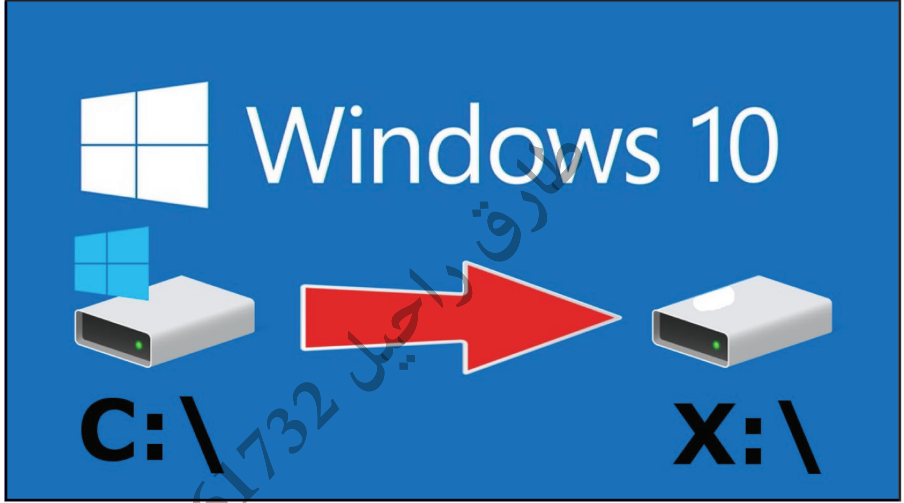
"on resume, display logon screen" کے چیک باکس کو چیک لگاتے ہوئے آپ اپنی پسند کا دورانیہ منتخب کر سکتے ہیں۔ اس فیچر کی افادیت اپنی جگہ لیکن اس کی قابلیت پر سوال اُٹھایا جاسکتا ہے کہ اگر فرض کریں آپ نے پانچ منٹس کا وقت متعین کیا ہے اور اس وقت سے پہلے کسی نے ماؤس کو ہلا دیا تو یہ وقت اب یہیں سے آگے پانچ منٹ تک پہنچ جائے گا۔ اس لیے اس مسئلے کو بالکل درست طریقے سے حل کرنے کے لیے مائیکروسافٹ ''ڈائنامک لاک'' (Dynamic Lock) کا آپشن پیش کرنے جا رہی ہے۔ یہ آپشن ونڈوز 10 کی خاص کری ایٹرز اپ ڈیٹس جو کہ اپریل 2017 میں جاری کی جائیں گی میں دیا جائے گا۔ جب آپ اس فیچر کو فعال کریں گے تو یہ ویب کیم کے ذریعے آپ کی تصویر محفوظ کر لے گا۔ اس کے بعد اگر یہ آپ کو کمپیوٹر کے سامنے نہ پائے گا تو فوراً اسکرین لاک کر دے گا۔ لیکن کتنی دیر بعد لاک کرے گا اور کیا یہ فیچر ''ونڈوز ہیلو'' کا حصہ ہوگا فی الحال اس طرح کی تمام تفصیلات آنا باقی ہیں۔

تاہم اس بات کا اندازہ ضرور لگایا جاسکتا ہے کہ ونڈوز 10 میں کئی زبردست اور اہم تبدیلیاں آنے کو ہیں۔



انسٹال پروگرامز کو ایک ڈرائیو سے دوسری ڈرائیو میں منتقل کریں

اکثر جب ایک ڈرائیو میں جگہ کم ہونے لگتی ہے تو ہم فائلز کو اُس ڈرائیو سے کسی دوسری ڈرائیو میں منتقل کر دیتے ہیں۔ لیکن مسئلہ تب بنتا ہے جب ہم دیکھتے ہیں کہ کئی انسٹال شدہ پروگرامز نے ایک بڑی اسپیس گھیر رکھی ہے اور ہم انھیں کہیں



دوسری جگہ منتقل نہیں کر سکتے، کیونکہ اس طرح وہ کام کرنا بند کر دیں گے۔ اگر آپ بھی کبھی اس صورتِ حال سے دوچار ہوں تو گھبرانے کی ضرورت نہیں، آئیے آپ کو بتاتے ہیں کہ کس طرح انسٹال شدہ پروگرامز کو ایک جگہ سے دوسری جگہ منتقل کیا جاسکتا ہے وہ بھی انتہائی آسانی کے ساتھ۔

ویسے تو اس کام کو بغیر کسی سافٹ ویئر کے بھی انجام دیا جاسکتا ہے لیکن اس میں وقت لگتا ہے اور کئی کمانڈز استعمال کرتے کئی مراحل کو مکمل کرنا پڑتا ہے۔ اس لیے اس کام کو آسان بنانے کے لیے آپ ''ایپلی کیشن موور'' (Application Mover) کا استعمال کر سکتے ہیں۔

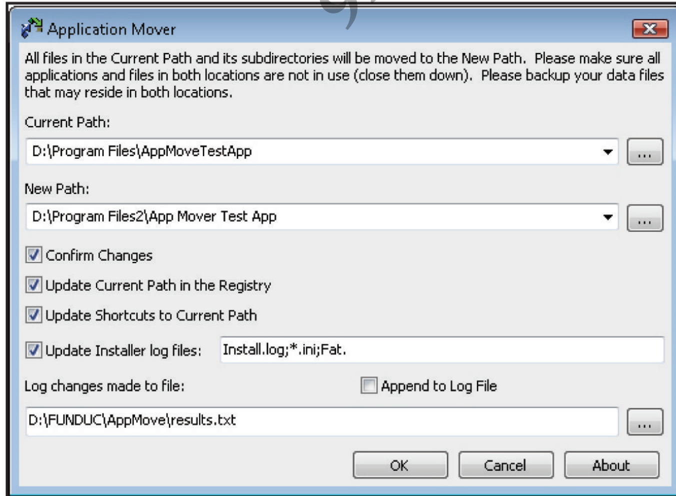
یہ پروگرام انسٹال شدہ پروگرام کو مکمل طور پر نئی جگہ منتقل کرسکتا ہے جس کے بعد وہ پروگرام بدستور پرانی صورت میں کام بھی کرتا رہتا ہے۔

ایپلی کیشن موور آپ ونڈوز وِستا، سیون، ایٹ اور ٹین پر بھی استعمال کر سکتے ہیں تاہم ڈاؤن لوڈ کرتے ہوئے اپنے آپریٹنگ سسٹم کے اعتبار سے 32 یا 64 بٹ ورژن ڈاؤن لوڈ کریں تاکہ یہ بالکل درست طریقے سے اپنا کام کر سکے۔

funduc.com/app_mover.htm

اس کے بعد اسے انسٹال کر کے چلائیں۔ سب سے پہلے جس پروگرام کو آپ منتقل کرنا چاہتے ہیں اس کا مقام منتخب کریں اس کے بعد اس کی نئی منزل بھی منتخب کریں۔ نیچے موجود چاروں چیک باکسز کو ضرور چیک رکھیں تاکہ یہ پروگرام کو منتقل کرتے ہوئے اس کی رجسٹری ایڈیٹر میں موجود اینٹریز کو بدل دے اس کے شارٹ کٹس کو بھی نئے مقام کا راستہ دِکھا سکے۔

یاد رکھیں کہ یہ پروگرامز کو مکمل منتقل کرتا ہے لیکن صرف سسٹم کی موجودہ ہارڈ ڈسک میں۔ اگر آپ کسی ایکسٹرنل ڈرائیو میں منتقلی کا کام انجام دیں گے تو پروگرام خراب ہو جائے گا۔



ونڈوز 10 میں نئے فیچرز قبل از وقت حاصل کریں

آج کل انٹرنیٹ کی دنیا میں ونڈوز 10 کی ’’کری ایٹرز اپ ڈیٹ‘‘ (Creators Update) کا بہت چرچا ہے۔ دراصل یہ خاص اپ ڈیٹ ہے جو کہ حتمی تیاری کے بعد اپریل 2017 میں جاری کی جائے گی۔ اس اپ ڈیٹ کے ذریعے ونڈوز 10 میں کئی نئے فیچرز متعارف کرائے جائیں گے۔ ان نئے کئی فیچرز کا احوال آپ کمپیوٹنگ کے اسی شمارے میں ملاحظہ کرسکتے ہیں۔ مائیکروسافٹ نے ان فیچرز کی آزمائش کا سلسلہ شروع کرتے ہوئے اس اپ ڈیٹ کو ونڈوز انسائیڈر پری ویو پروگرام (Windows Insider Preview program) کے تحت ڈاؤن لوڈ کرنے کے لیے بھی پیش کردیا ہے۔ دراصل ونڈوز انسائیڈر پری ویو پروگرام میں ونڈوز کے آزمائشی ورژنز کو فائنل ریلیز سے قبل پیش کیا جاتا ہے چونکہ یہ آزمائشی ورژنز ہوتے ہیں اس لیے ان میں خرابیاں بھی موجود ہوسکتی ہیں اس لیے انھیں براہِ راست صارفین کو بھیجنے سے قبل مائیکروسافٹ ونڈوز انسائیڈر پری ویو پروگرام جو کہ زیادہ تر آئی ٹی ماہرین استعمال کرتے ہیں میں متعارف کراتی ہے۔ ونڈوز انسائیڈر پری ویو پروگرام کو کوئی بھی درج ذیل ربط پر جاکر اپنے مائیکروسافٹ اکاؤنٹ کے ذریعے جوائن کرکے ونڈوز کی آزمائشی اپ ڈیٹس کو حاصل کرسکتا ہے۔

insider.windows.com

جیسا کہ ہم نے ذکر کیا کہ ونڈوز 10 کری ایٹرز اپ ڈیٹ کا آج کل بہت چرچا ہے تو اس اپ ڈیٹ کو Build 15002 میں فراہم کیا گیا ہے جو کہ ISO فائل کی صورت میں ونڈوز انسائیڈر پری ویو پروگرام کی ویب سائٹ پر فراہم کردی گئی ہے۔

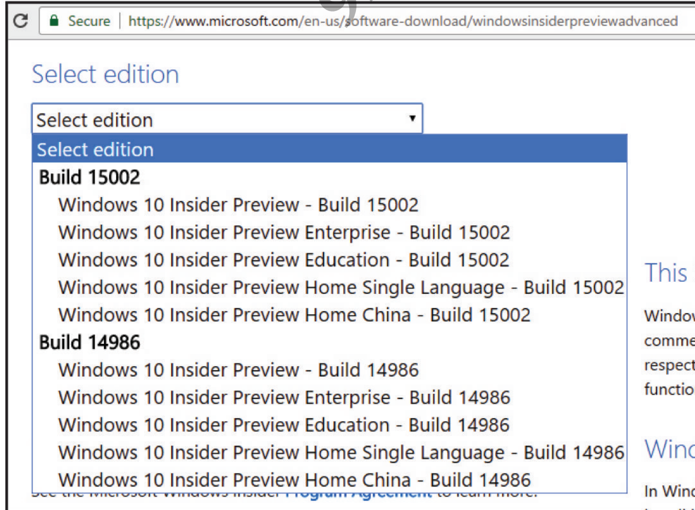
Build 15002 میں کئی نئے اور زبردست فیچرز پیش کیے گئے ہیں جیسے کہ ونڈوز کی اپ ڈیٹس کو عارضی طور پر بند کرنا، گیمز کھیلنے کے لیے خاص ’’گیم موڈ‘‘، ایج براؤزر، کورٹانا اور ونڈوز ڈیفینڈر کے نئے فیچرز وغیرہ۔ ان کے علاوہ بھی درجنوں نئے فیچرز اس اپ ڈیٹ کے ذریعے ونڈوز 10 کو ملیں گے۔

ونڈوز انسائیڈر پری ویو پروگرام کو جوائن کرنے کے بعد اس نئی اپ ڈیٹ کو آئی ایس او فائل کی صورت میں حاصل کرنے کے لیے درج ذیل ربط پر جائیں:

bit.ly/build15002

یہاں اس حوالے سے تمام تفصیل موجود ہے اور ڈراپ ڈاؤن لسٹ کے ذریعے آپ اپنی پسند کے آپریٹنگ سسٹم کے ساتھ یہ اپ ڈیٹ حاصل کرسکتے ہیں۔ یہ آئی ایس او فائل ڈاؤن لوڈ کرنے کے بعد آپ کو اس کی انسٹالیشن ڈِسک بنانا ہوگی۔ اس کے علاوہ یقیناً آپ جانتے ہوں گے کہ یہ ونڈوز کا آزمائشی ورژن ہے اور اس میں کئی خرابیاں ہوسکتی ہیں اور اس میں سامنے آنے والے مسائل یہ ونڈوز مائیکروسافٹ کو بھی ارسال کرتی رہے گی۔ اس لیے براہِ راست اپنے پی سی پر اس کی انسٹالیشن سوچ سمجھ کر کریں۔ اگر آپ ونڈوز کے نئے فیچرز کو دیکھنا چاہتے ہیں تو بہتر ہوگا پہلے اسے کسی ورچوئل مشین پر انسٹال کریں۔

اسے انسٹال کرنے کے لیے آپ کے پاس پہلے سے ایکٹی ویٹ شدہ ونڈوز 10 انسٹال ہونی چاہیے جو کہ اس اپ ڈیٹ کو استعمال کرتے ہوئے اپ گریڈ ہوگی۔



مستقبل کا اینٹی وائرس مفت حاصل کریں

لگتا ہے آخر کار اینٹی وائرس بنانے والی کمپنیز کو خیال آ ہی گیا ہے کہ لوگ کمپیوٹر صرف اس لیے استعمال نہیں کرتے کہ اس پر اینٹی وائرس انسٹال کر سکیں جو سسٹم کی پچاس سے ستر فیصد توانائیاں استعمال کرتے ہوئے ہارڈ ڈسک کو مسلسل مصروف رکھے اور سسٹم کو بالکل ہی سست بنا دے۔ اینٹی وائرس پروگرام وقت کے ساتھ ساتھ اس قدر بھاری بھر کم ہو چکے ہیں کہ اکثر لوگ اب انھیں انسٹال نا کرنے کو ہی ترجیح دیتے ہیں۔ یہی وجہ ہے کہ اینٹی وائرس بنانے والی کمپنیز اب اپنی مصنوعات کو کلاؤڈ سروسز کے ذریعے پیش کر رہی ہیں۔

اس فہرست میں تازہ ترین اضافہ ''میک ایفی کلاؤڈ اینٹی وائرس'' ہے۔ اس سے قبل ہم سوفوز کلاؤڈ اینٹی وائرس (Sophos) کا احوال بھی کمپیوٹنگ میں شائع کر چکے ہیں۔ کلاؤڈ اینٹی وائرس کی انسٹالیشن بہت ہی آسان ہوتی ہے اور اس کی زیادہ تر فائلز آپ کے سسٹم پر موجود نہیں ہوتیں اس لیے یہ نہ سسٹم ریسورسز کا طلب گار ہوتا ہے نہ ہی ہارڈ ڈسک پر زیادہ جگہ گھیرتا ہے۔

میک ایفی کلاؤڈ اینٹی وائرس کی بات کریں تو یہ صرف 2 ایم بی کی صورت میں دستیاب ہے البتہ انسٹالیشن کے وقت یہ کچھ مزید ڈیٹا ڈاؤن لوڈ کرتا ہے لیکن روایتی اینٹی وائرس کی طرح یہ ڈیٹا کئی سو ایم بی پر مشتمل نہیں۔ انسٹالیشن کے بعد بس اس کا آئی کن سسٹم ٹرے میں موجود رہتا ہے جس سے اسے آن یا آف کیا جا سکتا ہے۔

دراصل کلاؤڈ اینٹی وائرس کے کام کرنے کا طریقہ کار یہ ہوتا ہے کہ اس کا چھوٹا سا پروگرام سسٹم کی نگرانی کرتا رہتا ہے اور جیسے ہی کوئی مشکوک سرگرمی دیکھتا ہے وہ اسے نوٹ کر کے اپنی کلاؤڈ سروس کو بھیج دیتا ہے، وہاں اس کا جائزہ لے کر اس کا موازنہ وائرس سے کیا جاتا ہے۔ اگر یہ واقعی وائرس ہو تو کلاؤڈ سروس سسٹم میں موجود پروگرام کو ہدایت دیتی ہے کہ فوراً اس فائل کو پکڑ لیا جائے۔

عام طور پر اینٹی وائرس کی تمام فائلز سسٹم میں موجود ہوتی، جن کے ذریعے وہ کسی مشکوک فائل کو پہچان پاتے ہیں کہ وہ وائرس ہے یا نہیں۔ یہی وجہ ہے کہ اینٹی وائرس کا اپ ڈیٹ ہونا انتہائی ضروری ہوتا ہے تا کہ وہ تازہ ترین وائرسز کے بارے میں آگاہ ہو۔ اس کے لیے اینٹی وائرس کی اپ ڈیٹس تقریباً روزانہ کی بنیاد پر جاری کی جاتی ہیں اور ان کا سائز کئی ایم بی پر مشتمل ہوتا ہے لیکن کلاؤڈ سروس چونکہ آپ کے سسٹم میں موجود نہیں ہوتی اور اس کے ساتھ بذریعہ انٹرنیٹ رابطہ کیا جاتا ہے اس لیے آپ ہر وقت اپ ڈیٹڈ ہی ہوتے ہیں۔ چونکہ آج ہمارے پاس ہر جگہ انتہائی تیز انٹرنیٹ فراہم ہو چکا ہے اس لیے کلاؤڈ بیسڈ پروگرامز انتہائی تیزی سے مقبول ہو رہے ہیں۔

یاد رکھیں کلاؤڈ اینٹی وائرس استعمال کرنے کے لیے آپ کے پاس ہر وقت انٹرنیٹ کا چل رہا ہونا ضروری ہے تا کہ کسی بھی مشکوک سرگرمی کی صورت میں اینٹی وائرس اپنی کلاؤڈ سروس سے رابطہ کر سکے۔ اس کے علاوہ آپ جب چاہیں عام اینٹی وائرس کی طرح اس سے اپنا سسٹم بھی اسکین کر سکتے ہیں۔

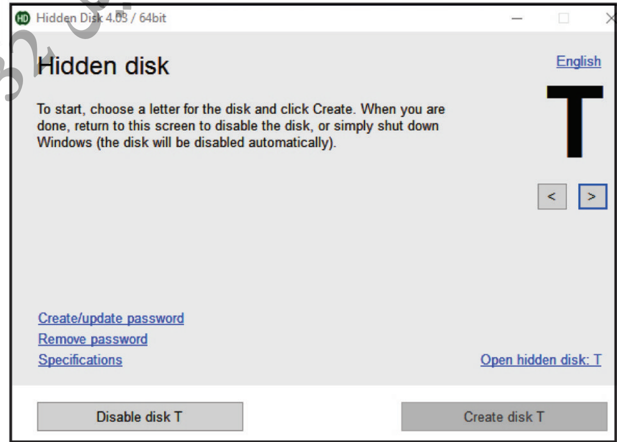
bit.ly/mcafeecloudav

پاس ورڈ کے ذریعے محفوظ ڈرائیو بنائیں

اکثر لوگ اپنے اہم ڈیٹا کی حفاظت کے لیے اسے پاس ورڈ کے ذریعے محفوظ فولڈرز میں رکھنا پسند کرتے ہیں۔ آیئے آپ کو بتاتے ہیں کہ کس طرح آپ ایک پاس ورڈ والی ڈرائیو اپنے کمپیوٹر میں بنا سکتے ہیں۔ اگر آپ کے پاس ''ہِڈن ڈِسک'' (Hidden Disk) پروگرام موجود ہو تو یہ کام چند منٹوں میں اور انتہائی آسانی کے ساتھ کیا جا سکتا ہے۔

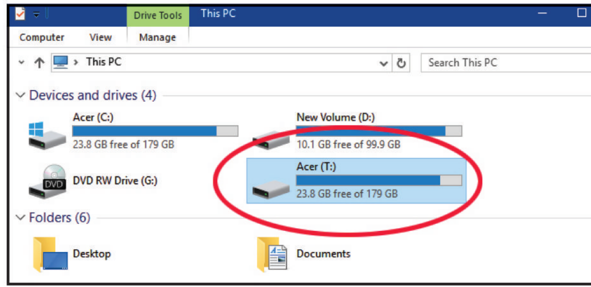
یہ پروگرام ونڈوز ایکس پی سے لے کر ٹین تک کے صارفین کے لیے صرف 2 ایم بی کے سائز میں بالکل مفت دستیاب ہے اور وہ بھی بغیر کسی قسم کے اشتہارات کے۔ اسے آپ درج ذیل ربط سے ڈاؤن لوڈ کر سکتے ہیں:

bit.ly/hiddis

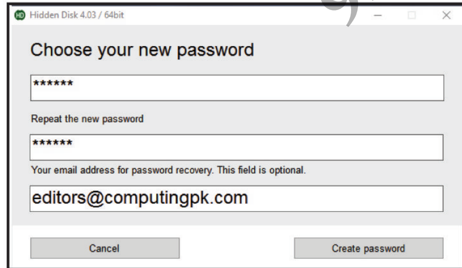


ڈاؤن لوڈ کرنے کے بعد اسے انسٹال کر لیں۔ انسٹالیشن مکمل ہونے کے بعد جب آپ اسے چلائیں گے تو یہ آپ کے لیے محفوظ ڈرائیو بنانے کے لیے تیار ہو گا۔ سب سے پہلے آپ کو ڈرائیو لیٹر منتخب کرنا ہے جیسے کہ سی اور ڈی ڈرائیو وغیرہ آپ کے سسٹم میں پہلے سے موجود ہوتی ہیں ان کے علاوہ کوئی ڈرائیو لیٹر منتخب کرنے کے بعد نیچے موجود ''کری ایٹ ڈسک'' (Create Disk) کے بٹن پر کلک کر دیں۔ اب آپ مائی کمپیوٹر کھول کر دیکھ سکتے ہیں کہ آپ کے منتخب کردہ لیٹر کے نام سے نئی ڈرائیو بھی موجود ہو گی۔

یہاں یہ بات یاد رکھنے کی اشد ضرورت ہے کہ دراصل یہ ڈرائیو آپ کی ونڈوز انسٹالیشن کی حامل ڈرائیو کے اندر ایک فولڈر ہے۔ اس لیے اس میں اتنی ہی اسپیس موجود ہو گی جتنی آپ کی ونڈوز ڈرائیو میں خالی ہو گی۔ اس کے علاوہ اس میں رکھا گیا ڈیٹا بیک اپ کرنے سے پہلے ونڈوز کو فارمیٹ یا ری انسٹال مت کریں ورنہ آپ کا یہ ڈیٹا ضائع ہو جائے گا۔



اب آپ اسی پروگرام کے ذریعے پاس ورڈ بھی منتخب کر سکتے ہیں۔ پاس ورڈ کم از کم چار ہندسوں کا ہونا چاہیے اس کے علاوہ اپنا ای میل ایڈریس دینا بھی ضروری ہے تا کہ پاس ورڈ بھولنے کی صورت میں اسے واپس حاصل کیا جا سکے۔ ان تمام سیٹنگز کے بعد اس ڈرائیو کو مائی کمپیوٹر سے غائب کرنے کے لیے ''ڈِس ایبل ڈِسک'' (Disable disk) کے بٹن پر کلک کریں تو یہ ڈرائیو غائب ہو جائے گی۔



اپنے پاس ورڈ کو آزمانے کے لیے اب اس پروگرام کو بھی بند کر کے دوبارہ کھولیں، اس دفعہ آپ سے پاس ورڈ طلب کیا جائے گا۔ درست پاس ورڈ درج کرتے ہی یہ پروگرام کھل جائے گا اور اپنی ڈرائیو کو سامنے لانے کے لیے آپ کو دوبارہ ''کری ایٹ ڈِسک'' کے بٹن پر کلک کرنا ہو گا۔ پروگرام کی ضرورت نہ رہنے پر ڈِس ایبل ڈِسک کرتے ہوئے اسے اَن اِنسٹال کر دیں۔

پی سی کو یو ایس بی کے ذریعے لاک یا اَن لاک کریں

اپنے سسٹم کو غیر ضروری چھیڑ چھاڑ سے محفوظ رکھنے کے لیے ہم سسٹم کو لاک کر دیتے ہیں تا کہ یہ آن رہے اور جب ہم واپس آئیں تو فوراً اسے اَن لاک کر کے اپنے کام کو جاری رکھ سکیں۔ کیا آپ جانتے ہیں کہ یو ایس بی فلیش ڈرائیو کے ذریعے بھی سسٹم کو لاک یا اَن لاک کیا جا سکتا ہے؟ اس کام کے لیے کئی پروگرامز موجود ہیں اور چند ایک کا ذکر ہم پہلے بھی کمپیوٹنگ میں کر چکے ہیں۔ اس بار ہم آپ کے لیے ایک نیا پروگرام پیش کر رہے ہیں کیونکہ یہ پروگرام استعمال میں انتہائی آسان ہے لیکن فیچرز سے بھرا ہوا ہے۔

ہماری روایت ہے کہ ہم صرف مفت پروگرامز کا ذکر کرتے ہیں لیکن یہ پروگرام مفت نہیں۔ اس کے باوجود اس کا احوال صرف اس لیے لکھا جا رہا ہے کیونکہ اس میں انتہائی کارآمد فیچرز موجود ہیں جو کہ ہمارے قارئین ہم سے فرمائش کرتے ہیں کہ کسی ایسے پروگرام کے بارے میں شائع کیا جائے۔

اس پروگرام کا نام ''پریڈیٹر'' (Predator) ہے۔ یہ صرف دس دن کے لیے مفت دستیاب ہے اس کے بعد اس کو خریدنا ہوگا۔ اسے استعمال کرنے کے لیے آپ کے پاس کوئی سی بھی یو ایس بی فلیش ڈرائیو یا ایس ڈی کارڈ موجود ہونا چاہیے۔ یہ پروگرام آپ درج ذیل ربط سے ڈاؤن لوڈ کر سکتے ہیں:

www.predator-usb.com

اس کی انسٹالیشن کے بعد آپ اپنی یو ایس بی کو پی سی میں لگا کر اُسے یہ اختیار دے سکتے ہیں کہ وہ آپ کے سسٹم کو لاک یا اَن لاک کر سکے۔ یوں سمجھیں کہ اس کے بعد جب تک یو ایس بی سسٹم میں منسلک رہے گی سسٹم چلتا رہے گا، جیسے ہی آپ یو ایس بی کو سسٹم سے نکالیں گے کی بورڈ اور ماؤس فوراً لاک ہو جائیں گے جبکہ اسکرین کالی ہو جائے گی۔ یعنی سسٹم استعمال کے قابل نہیں رہے گا۔ اس کے بعد جیسے ہی آپ یو ایس بی واپس سسٹم میں لگائیں گے پی سی دوبارہ فوراً واپس اصلی حالت میں آ جائے گا۔ اس میں پاس ورڈ بھی سیٹ کیا جاتا ہے تا کہ یو ایس بی کی غیر موجودگی میں بھی آپ سسٹم کو اَن لاک کر سکیں۔

اسے استعمال کرنے کے لیے ضروری ہے کہ آپ کی یو ایس بی فلیش ڈرائیو کا فائل سسٹم FAT32 ہو۔ اگر یہ این ٹی ایف ایس فائل سسٹم پر مشتمل ہو گی تو ایسی یو ایس بی اس پروگرام کے ساتھ استعمال نہیں کی جا سکتی، پہلے یو ایس بی کو FAT32 فائل سسٹم پر فارمیٹ کرنا ہوگا۔

یہ پروگرام آپ ونڈوز ایکس پی سے لے کر ونڈوز 10 تک پر استعمال کر سکتے ہیں، یہ 32 اور 64 بٹ آپریٹنگ سسٹم کے لیے الگ الگ ڈاؤن لوڈ کرنے کے لیے موجود ہے اس لیے ڈاؤن لوڈ کرتے وقت اس بات کا خیال رکھیں اور اپنے آپریٹنگ سسٹم کے اعتبار سے ڈاؤن لوڈ کریں۔

اس پروگرام کے اضافی فیچرز کی بات کی جائے تو آپ کی غیر موجودگی میں اگر کوئی سسٹم کو لاگ اِن کرنے کی کوشش کرے گا تو یہ اُس کی تصویر بنا سکتا ہے، ای میل کے ذریعے آپ کو الرٹس بھی بھیج سکتا ہے، ساؤنڈ الارم کے ذریعے بھی آپ کو خبردار کر سکتا ہے، ایک ہی یو ایس بی آپ کئی کمپیوٹرز کے لیے استعمال کر سکتے ہیں، یہ صرف چند کے بی کی فائل یو ایس بی میں رکھتا ہے اس کے بعد آپ یو ایس بی کو عام طریقے سے بدستور استعمال کر سکتے ہیں۔



2017 کی ٹاپ 5 ٹورینٹس ویب سائٹس

گزشتہ سال ٹورینٹس ویب سائٹ پر بڑا بھاری گزرا اور کئی نامور ٹورینٹس ویب سائٹس کو لے ڈوبا جیسے کہ ٹورینٹز (Torrentz) اور کیٹ (KAT)۔ ان دونوں بڑی ٹورینٹس ویب سائٹس کو پائریسی کے قانون کی خلاف ورزی کے جرم میں کارروائی کا نشانہ بنایا گیا۔ کیٹ ویب سائٹ واپس تو آ چکی ہے لیکن یہ پہلے جیسی شہرت کھو چکی ہے۔ اس کے علاوہ ویب سائٹ کے ڈاؤن ٹائم میں اس کی کئی جعلی کاپیز انٹرنیٹ پر دستیاب ہوگئیں جنھوں نے وائرس پھیلانے کا کام کیا۔ جس کی وجہ سے صارفین اب پہچان نہیں کر پاتے کہ کون سی ویب سائٹ اصلی ہے اور کون سی جعلی۔ اکثر ویب سائٹ درست طریقے سے کام بھی نہیں کرتی، یہی وجہ اس ویب سائٹ کی مقبولیت کو کم کرنے کی وجہ بنی۔

نیا سال شروع ہو چکا ہے اور کئی ٹورینٹس ویب سائٹس تا حال موجود ہیں۔ یہ ویب سائٹس الیکسا ورلڈ رینکنگ میں انتہائی اچھی جگہ رکھتی ہیں، یہ صرف ویب سائٹس ہی نہیں بلکہ کاروبار ہیں جو کہ ٹھیک ٹھاک پیسہ بنا رہی ہیں۔ آیئے آپ کو بتاتے ہیں کہ اس وقت کون کون سی ٹورینٹس ویب سائٹ سب سے مقبول ہیں۔

دی پائریٹ بے (The Pirate Bay)

یہ ویب سائٹ ٹورینٹس کی بادشاہ ہے اور پچھلے کئی سالوں سے اس میدان میں موجود ہے۔ گزشتہ سال یہ رینکنگ میں دوسرے نمبر پر موجود تھی لیکن اس سال یہ نمبر ون کے طور پر اُبھری ہے اور اس وقت ٹورینٹس کی سب سے بڑی ویب سائٹ ہے۔ دنیا بھر میں اس کی الیکسا رینکنگ 116 ہے۔

ایکسٹرا ٹورینٹ (ExtraTorrent)

حالیہ عرصے میں ایکسٹرا ٹورینٹ نے انتہائی تیزی سے مقبولیت کی سیڑھیاں چڑھی ہیں اور اس وقت یہ دوسری مقبول ترین ٹورینٹس ویب سائٹ بن چکی ہے جبکہ اس کی عالمی الیکسا رینکنگ میں بھی بہت بہتری آئی ہے اور اس وقت یہ 244 نمبر پر موجود ہے۔

آر اے آر بی جی (RARBG)

یہ ویب سائٹ ویسے تو 2008 میں شروع کی گئی تھی لیکن یہ کبھی زیادہ مقبولیت کو نہ پہنچ سکی۔ لیکن گزشتہ سال بڑی ٹورینٹس ویب سائٹس جب ڈاؤن ہوئیں تو ٹورینٹس کے متلاشی اس ویب سائٹ تک جا پہنچے۔ یہی وجہ ہے کہ اسے انتہائی تیزی سے مقبولیت حاصل ہوئی اور اب یہ تیسرے نمبر پر موجود ہے جبکہ اس کی عالمی الیکسا رینکنگ 272 ہے۔

وائے ٹی ایس (YTS)

وائے ٹی ایس جو کہ YIFY کے نام سے جانی جاتی ہے فلموں کے ٹورینٹس فراہم کرنے کے حوالے سے اس وقت ایک انتہائی مقبول ویب سائٹ ہے۔ اس کی خاصیت کم سائز میں عمدہ معیار کے ٹورینٹس فراہم کرنا ہے۔ اس ویب سائٹ کو بنانے والوں نے پہلے اپنے ٹورینٹس دوسری ویب سائٹس پر اپ لوڈ کر کے مقبولیت حاصل کی اور بعد میں اپنا پروجیکٹ شروع کیا جو کہ بڑی ویب سائٹس کے ڈاؤن ٹائم میں فوراً مقبولیت حاصل کر گیا۔

اس وقت یہ ویب سائٹ ٹورینٹس کی دنیا میں چوتھے جبکہ عالمی الیکسا رینکنگ میں 335 نمبر پر موجود ہے۔

ون تھری تھری سیون ایکس (1337X)

اس انتہائی نامقبول بلکہ نامعقول ویب سائٹ نے بھی گزشتہ سال اسی طرح فائدہ اُٹھاتے ہوئے رینکنگ میں بہتری حاصل کی اور اس وقت یہ پانچویں بڑی ٹورینٹس ویب سائٹ کے طور پر اُبھری ہے۔ جبکہ عالمی الیکسا رینکنگ میں یہ 819 نمبر پر موجود ہے۔

گیم تمام سیٹنگز اور پروگریس کے ساتھ بیک اپ کریں

اسمارٹ فون گیم کھیلنا سبھی کو پسند ہوتا ہے۔ ہم گھنٹوں ان گیمز پر صرف کرتے ہیں اور آگے سے آگے بڑھتے جاتے ہیں لیکن تشویش اس وقت ہوتی ہے جب ہمارے فون میں کوئی خرابی ہو جاتی ہے اور اسے فیکٹری سیٹنگز پر ری سیٹ کرنا پڑ جاتا ہے۔ یا پھر آپ پرانا فون چھوڑ کر نئے فون پر منتقل ہونا چاہتے ہیں لیکن اس صورت میں آپ کی کھیلی گئی گیم کی تمام پروگریس پرانے فون میں ہی رہ جاتی ہے اور سارا گیم دوبارہ سے کھیل کر اُسی مقام تک پہنچنا پڑتا ہے۔

اس مسئلے کو بڑی خوبصورتی کے ساتھ ''ہیلیئم'' (Helium) بیک اپ ایپلی



کیشن کے ذریعے حل کیا جا سکتا ہے۔ اس ایپلی کیشن کے ذریعے آپ فون کو روٹ کیے بغیر تمام ڈیٹا بشمول ایپ ڈیٹا کو ایس ڈی کارڈ، کمپیوٹر یا کلاؤڈ اسٹوریج پر نہ صرف بیک اپ کر سکتے ہیں بلکہ بوقت ضرورت یعنی ڈیوائس بدلنے کے بعد ری اسٹور بھی کر سکتے ہیں۔

فرض کریں آپ ایک گیم کو بیک اپ کرنا چاہتے ہیں تا کہ اسے نئے فون پر منتقل کر سکیں تو اس کے لیے سب سے پہلے آپ کو ہیلیئم ایپلی کیشن اپنے فون پر انسٹال کرنا ہوگی۔ اگر آپ یہ بیک اپ ایس ڈی کارڈ پر کریں تو انتہائی آسان ہے کہ بیک اپ کرنے کے بعد ایس ڈی کارڈ کو نئے فون میں لگائیں اور وہاں بھی ہیلیئم انسٹال کر کے اس بیک اپ کو ری اسٹور کر لیں۔ فرض کریں آپ کے نئے یا پرانے فون میں ایس ڈی کارڈ کی سہولت موجود نہیں تو یہ کام بذریعہ کلاؤڈ بیک اپ یا پی سی کے ذریعے بھی کیا جا سکتا ہے۔

اس کے لیے سب سے پہلے ہیلیئم کا ڈیسک ٹاپ ورژن درج ذیل ربط سے ڈاؤن لوڈ کر کے انسٹال کر لیں:

bit.ly/heliumdesktop

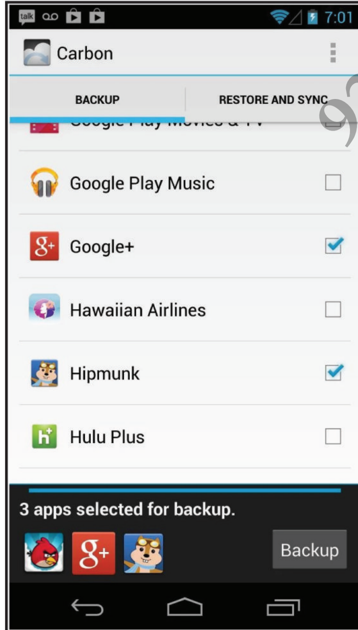
اب اپنے اینڈرائیڈ فون پر بھی ہیلیئم گوگل پلے اسٹور سے انسٹال کر لیں:

bit.ly/heliumapp

ہیلیئم کا مفت ورژن آپ کے لیے کافی ہے لیکن اگر آپ بیک بذریعہ کلاؤڈ اسٹوریج کرنا چاہتے ہیں تو اس کے لیے ایپ کا پریمیئم ورژن درکار ہوگا جو کہ 5 امریکی ڈالر میں دستیاب ہے۔

پہلے تو یہ اچھی طرح سمجھ لیں کہ بنیادی طور پر یہ ایک بیک اپ ایپلی کیشن ہے جو آپ کے فون کو بیک اپ کرنے کے لیے ہر طرح کی صلاحیت سے لیس ہے۔ مثلاً فون کلاؤڈ اسٹوریج پر بیک اپ کرنا ہو، پی سی پر بیک اپ کرنا ہو چاہیے بذریعہ یو ایس بی کیبل یا وائی فائی، بذریعہ کروم براؤزر بیک اپ کرنا ہو اس میں تمام فیچرز موجود ہیں۔

مطلوبہ گیم یا کسی بھی ایپلی کیشن کو ایک جگہ سے بیک اپ کرنا ہے اور پھر اس بیک کو نئے فون میں لے جانا ہے یا اسی فون میں آپ جب چاہیں ری اسٹور کر سکتے ہیں۔

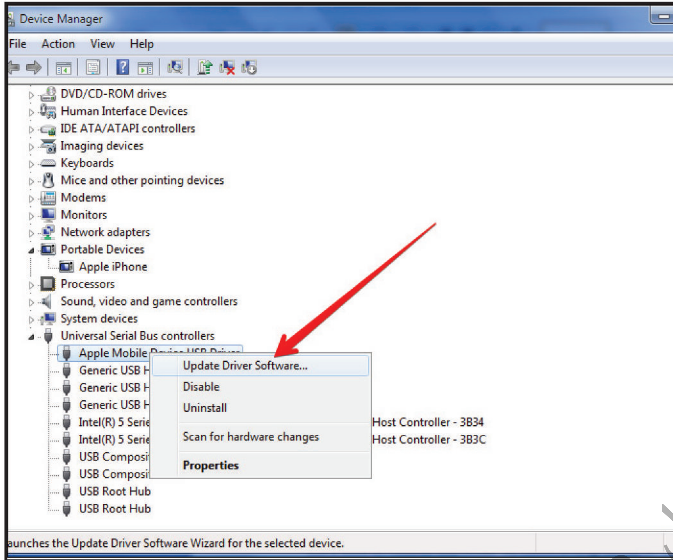


ونڈوز فائل ایکسپلورر میں آئی فون کا دِکھائی نہ دینا ٹھیک کریں

ایک وقت تھا جب آئی فون اور مسائل کا زیادہ تعلق نہیں تھا۔ آئی فون صارفین بڑے سکون سے اپنا فون استعمال کرتے تھے کیونکہ انھیں اینڈرائیڈ صارفین کی طرح آئے دن نت نئے مسائل کا سامنا نہیں کرنا پڑتا تھا، لیکن وہ اچھا دور اسٹیو جابز کے دنیا سے جانے کے ساتھ ہی رخصت ہو چکا ہے۔ اب آئی فون صارفین بھی آئے دن نت نئے مسائل کا شکار رہتے ہیں۔ ان میں سے ایک مسئلہ بڑا اہم ہے جس میں آئی فون ونڈوز فائل ایکسپلورر میں نظر نہیں آتا۔

آئی فون اور ونڈوز پی سی کے درمیان ڈیٹا کا تبادلہ کرنا ایک روزمرہ کا عمل ہے لیکن صارفین کو ونڈوز 10 میں آئی فون کنیکٹ کرنے میں آج کل دشواری کا سامنا ہے۔ اب جب اس میں دو مختلف پارٹیاں موجود ہیں یعنی ایک طرف مائیکروسافٹ اور دوسری طرف ایپل، جو کہ کبھی ایک دوسرے کی اچھی دوست نہیں رہیں تو اس مسئلے کا پائیدار حل سامنے نہیں آ رہا، کیونکہ دونوں ہی اس مسئلے کی وجہ ایک دوسرے کو قرار دیتے ہیں۔

بہرحال اگر آپ اس مسئلے کا سامنا کر رہے ہیں تو آئیے آپ کو بتاتے ہیں کہ کس طرح اسے ٹھیک کرنے کی کوشش کی جا سکتی ہے۔

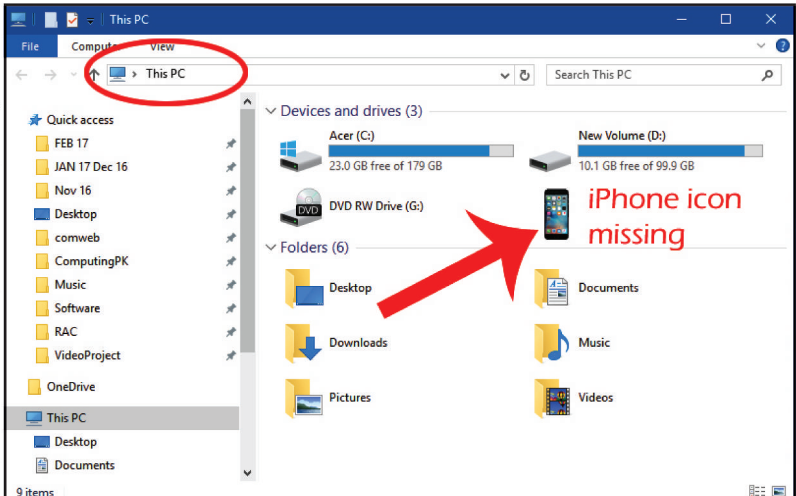


آئی فون کو پی سی کے ساتھ یو ایس بی کیبل کے ذریعے کنیکٹ کریں اور اس کے بعد درج ذیل طریقے آزمائیں:

ڈیوائس منیجر میں جا کر Apple Mobile Device USB Driver کو اپ ڈیٹ کریں۔ ونڈوز خود بخود ڈرائیور کی اپ ڈیٹس بذریعہ انٹرنیٹ تلاش کر کے انسٹال کر سکتی ہے۔

اگر یہ طریقہ کام نہ کرے تو ایک دفعہ ڈرائیور کو مکمل طور پر اَن انسٹال کر کے پی سی کو ری اسٹارٹ کر کے دوبارہ فون کنیکٹ کریں۔ اب ونڈوز دوبارہ ڈرائیور کو تازہ انسٹال کرنے کی کوشش کرے گی۔

فون کو پی سی سے کنیکٹ کرنے کے لیے آئی ٹیونز کا بھی بہت بڑا عمل دخل ہوتا ہے۔ اگر یہ مسئلہ بدستور موجود رہے تو ایپل کی ویب سائٹ سے آئی ٹیونز کا تازہ ورژن ڈاؤن لوڈ کر کے اِنسٹال کریں۔ ان تینوں طریقوں کو استعمال کرنے سے یہ مسئلہ حل ہو جانا چاہیے۔



یوٹیوب پر لاگ اِن کیے بغیر بلاک وڈیوز دیکھیں

یوٹیوب کی پالیسی ہے کہ اگر کسی وڈیو میں ایسا مواد موجود ہو جو عام ناظرین کے لیے مناسب نہ ہو تو ناظر کو پہلے خبردار کیا جاتا ہے۔ کم عمر افراد کو ایسی وڈیوز سے دُور رکھنے کے لیے یوٹیوب پر گوگل اکاؤنٹ سے لاگ اِن کرنے کا کہا جاتا ہے تاکہ صارف کی عمر کا پتا لگایا جا سکے۔ چونکہ گوگل اکاؤنٹ میں صارف کی تاریخ پیدائش درج ہوتی ہے اس لیے وہاں سے تصدیق کرنے کے بعد وڈیو دیکھنے کی اجازت دی جاتی ہے۔

فرض کریں آپ کوئی ایسی وڈیو دیکھنا چاہتے ہیں جو کہ جانتے ہیں کہ ایسے خطرناک مناظر کی حامل نہیں ہے اور اُسے دیکھنا آپ کے لیے ضروری ہے لیکن آپ اپنے گوگل اکاؤنٹ سے لاگ اِن ہونا بھی نہیں چاہتے تو اس کا ایک بہت ہی آسان سا حل موجود ہے جس کے لیے آپ کو کوئی بھی سافٹ ویئر یا پلگ اِن درکار نہیں۔

اس کے لیے بس آپ کو یوٹیوب کے URL میں تبدیلی کرنی ہوگی۔ یقیناً آپ جانتے ہوں گے کہ ہر یوٹیوب وڈیو کی ایک خاص آئی ڈی ہوتی ہے جو کہ یوآرایل کے اختتام پر موجود ہوتی ہے۔ جیسے کہ درج ذیل ربط پر غور کریں:

www.youtube.com/watch?v=Espy9UznCMw

اس میں آپ دیکھیں کہ = کے بعد آئی ڈی موجود ہے۔ اس ربط میں آپ نے بس watch?v= کو /v سے بدلنا ہے جیسے کہ اب یہ ربط دیکھیں:

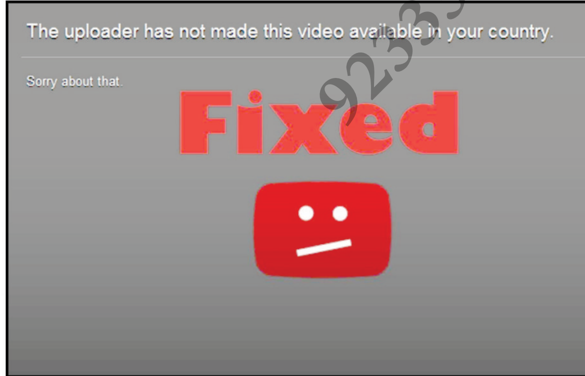


www.youtube.com/v/Espy9UznCMw

جب آپ اس ربط کو استعمال کریں گے تو وڈیو بغیر لاگ اِن کیے کھل جائے گی۔



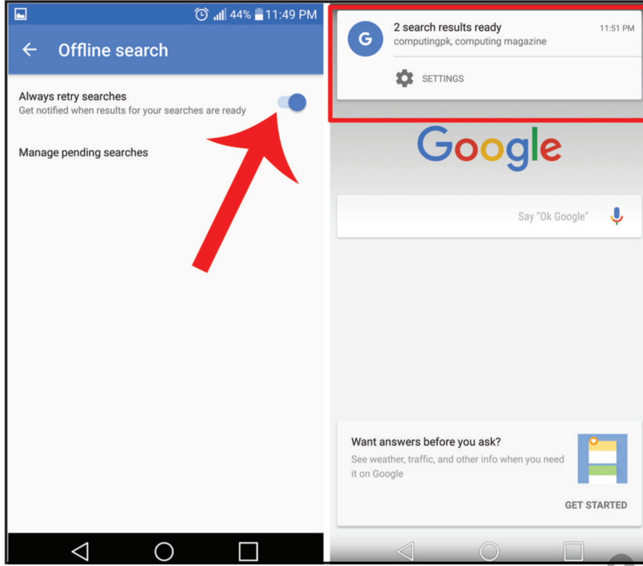
اس کے علاوہ اکثر آپ نے دیکھا ہوگا کہ وڈیو اپ لوڈ کرنے والے اس پر جغرافیائی حدود بھی لاگو کردیتے ہیں یعنی کہ یہ وڈیو صرف فلاں ملک میں دیکھی جا سکتی یا فلاں ملک میں نہیں دیکھی جا سکتی۔



ایسی وڈیوز کو دیکھنے کے لیے آپ ''پراکس ٹیوب'' ایڈ اون انسٹال کرسکتے ہیں جو کہ گوگل کروم اور موزیلا فائرفوکس کے لیے مفت دستیاب ہے۔ اپنے براؤزر میں اسے انسٹال کرنے کے لیے درج ذیل ربط ملاحظہ کریں:

proxtube.com

گوگل کا نیا فیچر ''آف لائن سرچ'' استعمال کرنا سیکھیں



انٹرنیٹ پر تلاش کرنے کا نام اب ''گوگل کرنا'' ہو چکا ہے۔ اس بات میں کوئی شک نہیں کہ گوگل انٹرنیٹ سرچنگ کا بادشاہ ہے۔ اسمارٹ فونز کی آمد کے بعد گوگل کی افادیت میں مزید اضافہ ہوگیا ہے کہ جہاں کہیں کوئی بات یاد نہ آرہی ہو یا کسی قسم کی معلومات درکار ہو، ہم فوراً گوگل کا رُخ کرتے ہیں اور سیکنڈوں میں معلومات تلاش کرلیتے ہیں۔

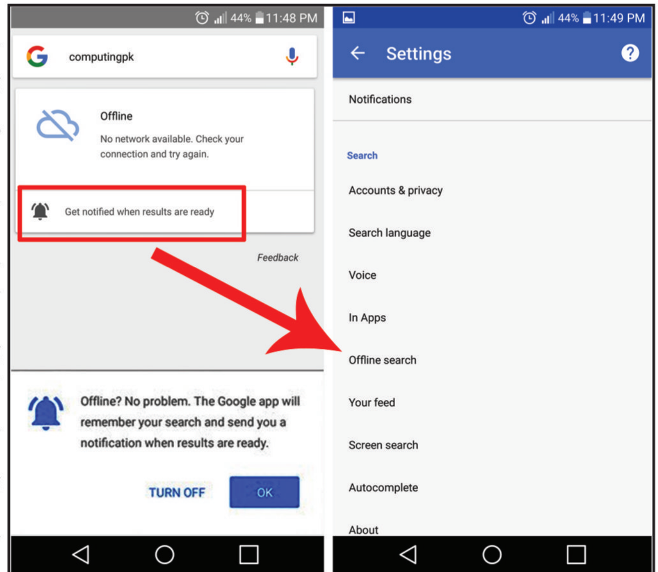
اینڈرویڈ میں گوگل نے ایک نیا فیچر متعارف کرایا ہے جسے استعمال کرتے ہوئے آپ آف لائن سرچز کو بعد میں آن لائن سرچ کرنے کے لیے محفوظ کرسکتے ہیں۔

فرض کریں کسی وقت آپ نے گوگل پر کچھ تلاش کیا لیکن اس وقت آپ کے پاس انٹرنیٹ موجود نہیں تھا تو عموماً آپ کچھ دیر بعد جب انٹرنیٹ دستیاب ہوگا تو اُس بات کو بھول چکے ہوں گے کہ تھوڑی دیر پہلے کیا تلاش کرنا چاہتے تھے۔ لیکن گوگل کے ہوتے ہوئے ایسا ممکن نہیں۔ گوگل کا یہ نیا فیچر آف لائن ہونے کی صورت میں اس تلاش کو اپنے پاس محفوظ کر لے گا اور جیسے ہی انٹرنیٹ دستیاب ہوگا فوراً اسے تلاش کرکے سامنے پیش کردے گا۔

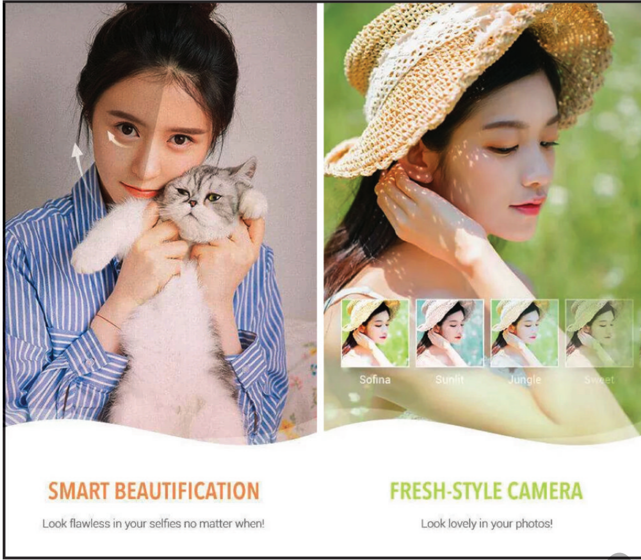
گوگل کا یہ کارآمد فیچر پہلے سے فعال ہوتا ہے اگر آپ اسے آزمانا چاہتے ہیں تو اینڈرویڈ فون یا ٹیبلٹ میں گوگل کھول کر کچھ تلاش کریں لیکن اس سے پہلے اپنا انٹرنیٹ بند کردیں۔

اب آپ دیکھیں گے گوگل جب انٹرنیٹ نہ ہونے کے سبب تلاش نہیں کر پائے گا تو فوراً یہ مشورہ دے گا کہ آپ کی یہ تلاش محفوظ کی جاسکتی ہے تاکہ انٹرنیٹ دستیاب ہوتے ہی فوراً آپ کو مطلع کیا جاسکے۔

''آف لائن سرچ'' کا آپشن یہیں سیٹنگز کے اندر موجود ہے جسے آپ جب چاہیں فعال یا غیر فعال کرسکتے ہیں۔ جیسا کہ ہم نے ذکر کیا کہ یہ آپشن پہلے سے فعال ہوتا ہے۔ اس لیے آپ کی یہ آف لائن سرچ محفوظ کردی جائے گی۔ اب اسے آزمانے کے لیے گوگل بند کردیں اور اپنا انٹرنیٹ آن کر لیں۔ آپ دیکھیں گے کہ فوراً ہی ایک نوٹی فکیشن کے ذریعے آپ کو مطلع کیا جائے گا کہ آپ کی تلاش تیار ہے، اس نوٹی فکیشن کے ذریعے آپ باآسانی اپنی مطلوبہ تلاش کے نتائج ملاحظہ کرسکتے ہیں۔ اس طرح تمام آف لائن سرچز کو گوگل محفوظ رکھتا ہے۔



اپنی عام تصویروں کو دیں ماڈل لُک وہ بھی ایک ٹچ سے



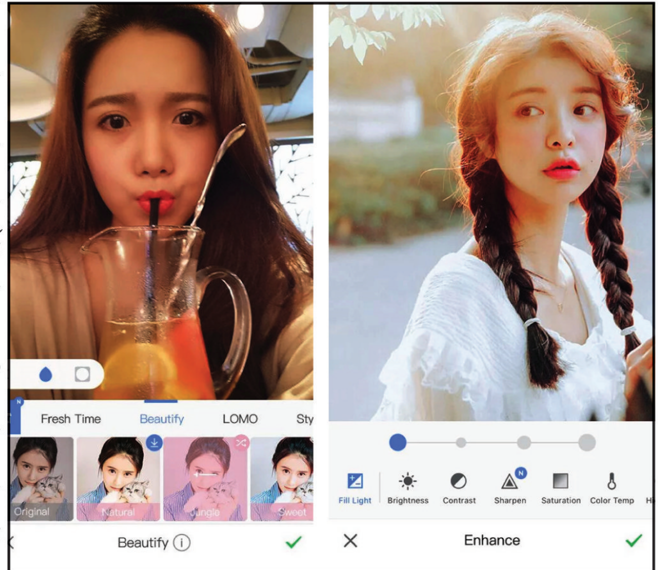
اپنی تصویروں کو خوبصورت بنانے کے لیے سبھی مختلف اپلی کیشنز استعمال کرتے ہیں، جن میں موجود فلٹرز ان کو خوبصورت بنا دیتے ہیں۔ اگر تصویر بناتے ہوئے کوئی کمی رہ گئی ہو، جیسے کہ آنکھوں کے نیچے حلقے نظر آرہے ہوں، چہرہ بہت موٹا نظر آرہا ہو یا آنکھیں چھوٹی ہوگئی ہوں، ان سب کو آج کل ایک ٹچ سے بدلا جاسکتا ہے۔ ویسے تو اس حوالے سے کئی اپلی کیشنز موجود ہیں لیکن چینی اپلی کیشن ''میتو'' (Meitu) کا کوئی جواب نہیں۔

میتو اپلی کیشن ویسے تو کئی سالوں سے ایشیا میں دستیاب تھی لیکن اسے اصل شہرت اب جا کر حاصل ہوئی ہے جب اسے یورپ کے لیے ریلیز کیا گیا ہے۔ اس اپلی کیشن نے مارکیٹ میں آتے انتہائی تیزی سے مقبولیت حاصل کی ہے اور ٹاپ ٹین ایپس میں جا کر شامل ہوگئی ہے۔

میتو اپلی کیشن کا پورا نام ''میتو شیو شیو'' ہے جس کا مطلب ہے ''خوبصورت تصویر مزید خوبصورت''۔ یہ اپلی کیشن اینڈرائیڈ اور آئی او ایس دونوں کے لیے بالکل مفت دستیاب ہے۔ اس میں اوپر ذکر کیے گئے تمام فیچرز موجود ہیں جن کو استعمال کرتے ہوئے آپ اپنی عام تصویر کو بھی ماڈل لُک دے سکتے ہیں۔

یہ اپلی کیشن چہرے کو خوبصورت بنانے میں اس لیے کامیاب رہتی ہے کیونکہ اس میں بہترین فیشل ریکگنیشن ٹیکنالوجی استعمال کی گئی ہے جو کہ 171 پوزیشننگ پوائنٹس سے چہرے کو بالکل درست انداز میں سمجھ کر فلٹرز استعمال کرتی ہے، یعنی یہ جانتی ہے کہ آنکھیں کہاں ہیں اس لیے اگر آپ آنکھیں بڑی یا چھوٹی کرنا چاہیں گے تو چہرہ بالکل بھی بدنما نہیں ہوگا۔ اسی طرح اگر آپ جِلد کو خوبصورت بنانا چاہیں گے تو یہ چہرے پر موجود داغ دھبے غائب کر دیتی ہے، بالوں کو بھی درست کرسکتی ہے۔ غرض ہر طرح کی سہولت اس میں موجود ہے جس سے عام تصویر کو خاص بنایا جاسکتا ہے۔

اکثر سکیورٹی ماہرین نے اس ایپ کو استعمال کرنے سے منع بھی کیا کہ آپ کی ذاتی معلومات جیسے مقام، فون نمبر اور EMIE نمبر وغیرہ نوٹ کر کے واپس چین بھیجتی ہے اور یہ ڈیٹا فروخت کیا جاتا ہے۔ جبکہ دیگر ماہرین کا کہنا ہے کہ یہ کوئی نئی بات نہیں ہے دیگر ایپس بھی ایسا کرتی ہیں۔ یہی بھی کہا جارہا ہے کہ دراصل یہ صرف اپلی کیشن کا ٹریکنگ مسئلہ ہے جاسوسی نہیں۔ تاہم میتو انتظامیہ نے اس الزام کو رد کیا ہے کہ ہم کسی کا ڈیٹا فروخت نہیں کرتے۔





کمپیوٹنگ کوئز

درج ذیل آسان سوالوں کے جوابات دے کر آپ حاصل کرسکتے ہیں، **2000** روپے تک کا کیش پرائز

1) وہ کون سی معروف ٹیکنالوجی کمپنی ہے جو نیویارک اسٹاک ایکسچینج میں **STX** کہلاتی ہے؟

☆ سونی ☆ سی گیٹ ٹیکنالوجیز ☆ سیلیکان ٹیکنالوجیز

2) One Laptop Per Child کس شخصیت کا منصوبہ ہے؟

☆ شہباز شریف ☆ بل گیٹس ☆ نیکولس نیگروپونتے

3) ہم یہ تو جانتے ہیں کہ دنیا کا پہلا کمپیوٹر وائرس "برین" دو پاکستانی بھائیوں کی ایجاد ہے، لیکن کیا آپ یہ بتا سکتے ہیں کہ کمپیوٹر وائرس کو یہ نام "وائرس" دراصل دیا کس نے ہے؟

☆ ڈاکٹر فریڈ کوہن ☆ ڈینس رچی ☆ گورڈن مور

☆......کوپن پر جوابات لکھ کر اس کوپن کی اسکین کاپی یا موبائل سے فوٹو کھینچ کر بھی بھیجا جاسکتا ہے۔

☆......موصول ہونے والے ای میل پیغامات چونکہ بہت زیادہ ہوتی ہیں، اس لئے کوپن مل جانے کی اطلاع دینا ہمارے لئے ممکن نہیں۔

پہلا انعام 2000 روپے نقد	(ایک انعام)
دوسرا انعام 200 روپے نقد	(10 انعامات)

شمارہ نمبر 124 کے سوالات کے درست جوابات

1: جِف 2: صحیح

3: کارل ساگان

پہلا انعام

وسیم بھٹی، سرگودھا

دوسرا انعام جیتنے والے دس قارئین

☆ محمد حنیف، ساہیوال ☆ فیروز صدیقی، کراچی ☆ نوید انجم، لاہور ☆ عمار احمد، لاہور ☆ زاہد رضوان، حیدرآباد ☆ سید عبیداللہ، پشاور ☆ محمد شفیق، کراچی ☆ وقار افضل، فیصل آباد ☆ عثمان، راولپنڈی ☆ عبدالرحیم کھوسو، لاڑکانہ

انعامی کوپن برائے شمارہ نمبر 125

جوابات: 1) .... 2) .... 3) ....

نام .... فون نمبر ....

پتا ....

....

یہ کوپن crm@computingpk.com پر ای میل کیجیے یا "ماہنامہ کمپیوٹنگ"، پوسٹ باکس نمبر 786، کراچی 74200 پر بذریعہ ڈاک ارسال کیجیے

مشتری ہوشیار باش!

گوگل پلے اسٹور پر جعلی ایپلی کیشنز پھیل رہی ہیں

پوری دنیا میں اسمارٹ فون کے بڑھتے استعمال کے ساتھ سوشل نیٹ ورکنگ سائٹس کو بھی استعمال کیا جاتا ہے۔ ایسے میں جہاں بڑی مقدار میں جعلی اکاؤنٹس دیکھے جاتے ہیں اب جعلی اکاؤنٹس کے ساتھ ساتھ سوشل نیٹ ورکنگ سائٹس کی جعلی اور وائرس سے آلودہ ایپس بھی گوگل پلے اسٹور پر پہنچ چکی ہیں جن کا استعمال کرنا آپ کے لئے خطرناک ثابت ہوسکتا ہے۔

گوگل پلے اسٹور پر معروف ترین ایپلی کیشنز جیسے کہ وٹس ایپ، فیس بک، یوٹیوب، گوگل اپ ڈیٹ، انسٹاگرام، نیٹ فلیکس، ہیک وائی فائی، ایئرڈرائیڈ، وائی فائی ہیکر، فوٹو شاپ، اسکائی ٹی وی، ہاٹ اسٹار، ٹرمپ ڈیش اور پوکے مون گو کے جعلی ورژن سامنے آئے ہیں۔ یہ ایپلی کیشنز ڈاؤن لوڈ کرنے سے پہلے تک آفیشل ایپلی کیشن کی طرح لگ رہی ہوتی ہیں اور بعض ایپلی کیشن بالکل آفیشل ایپلی کیشن کی طرح چل بھی رہی ہوتی ہیں۔ لیکن پس پردہ آپ کی ڈیوائس کا کنٹرول اور آپ کا ذاتی ڈیٹا ہیکروں کے حوالے کیا جاچکا ہوتا ہے۔

Zscaler کے آئی ٹی سکیوریٹی ریسرچرز نے گوگل پلے اسٹور پر ان جعلی ایپس کی نشاندہی کی گئی ہے جن میں اینڈرائیڈ صارفین کو پھنسانے کے لیے اسپائی نوٹ ریٹ (SpyNote RAT) تکنیک کا استعمال کیا گیا ہے۔ اس ٹروجن پر گزشتہ سال اگست میں رپورٹس سامنے آئی تھیں، جس سے پتا چلا کہ یہ ٹروجن جس اینڈرائیڈ کو نشان بناتا ہے اس پر ہیکر قبضہ کرسکتے ہیں۔

ان ایپس کے ذریعے فیس بک، وٹس ایپ، انسٹاگرام پر شیئر کی گئی آپ کی ذاتی معلومات کو آسانی سے وائرس کے ذریعے چرایا جاسکتا ہے۔ اپنی رپورٹ میں Zscaler کے آئی ٹی سیکورٹی ریسرچرز نے انکشاف کرتے ہوئے کہا ہے کہ اس وقت بہت سی دیگر فرضی ایپس بھی اس وائرس میں مبتلا ہیں، جن میں سپر ماریو رن اور پوکے مون گو سمیت کئی سوشل نیٹ ورکنگ سائٹس کی ایپس شامل ہیں۔ یہ وہی ایپلی کیشنز ہی جنہیں لوگ سب سے زیادہ ڈاؤن لوڈ کرتے ہیں۔

اسی طرح یہ ایپس گوگل پلے اسٹور کے علاوہ تھرڈ پارٹی ویب سائٹس پر بھی موجود ہیں۔ گوگل پلے اسٹور پر تو اصل اور نقل ایپ میں تمیز کی جاسکتی ہے لیکن تھرڈ پارٹی ویب سائٹ پر یہ ممکن نہیں رہتا۔ اس لیے بہتر ہے کہ ہمیشہ ایپ گوگل پلے اسٹور سے ڈاؤن لوڈ کریں اور ڈاؤن لوڈ کرنے سے پہلے اس کے ڈیولپر کا نام ضرور دیکھ لیں۔ یاد رکھیں کہ فیس بک یا وٹس ایپ سے متعلقہ کوئی بھی ایپلی کیشن صرف فیس بک یا وٹس ایپ ہی جاری کرے گا۔ اگر کوئی abc کمپنی فیس بک جیسے لوگو اور نام والی کوئی ایپلی کیشن پلے اسٹور یا اپنی ویب سائٹ پر ڈاؤن لوڈنگ کے لئے فراہم کررہی ہے تو وہ سو فیصد جعلی اور خطرناک ہے۔

بیرونی ذرائع (یعنی گوگل پلے اسٹور کے علاوہ کسی بھی ویب سائٹ) سے کوئی بھی ایپ انسٹال مت کریں اور خاص طور پر اگر کوئی آپ کو کسی ایپ کا لنک بذریعہ پیغام یا ای میل دے تو اسے تو بالکل بھی مت انسٹال کریں۔ ورنہ آپ اپنا نجی ڈیٹا ہیکروں کے رحم و کرم پر چھوڑ دیں گے! ■



گرافک ڈیزائننگ، ویڈیو ایڈیٹنگ اور پوسٹ پروڈکشن کے میدان میں جناب عمران شہزاد کا نام کسی تعارف کا محتاج نہیں۔ آپ اس شعبے میں گزشتہ پندرہ سال سے کام کر رہے ہیں اور اس دوران مختلف تعلیمی و تربیتی اداروں سے بطور استاد وابستہ رہے ہیں۔ مارفنگ، ٹوٹل ویڈیو کنورٹر اور گرافکس/ملٹی میڈیا سے متعلق کئی سافٹ ویئر کے بارے میں آپ کی متعدد عملی اور ماہرانہ تحریریں ماہنامہ کمپیوٹنگ کے صفحات پر شائع ہوتی رہی ہیں؛ جنہیں قارئین نے بے حد سراہا ہے۔ جناب عمران شہزاد کے زیرِ نگرانی ''ہاؤس آف گرافکس'' (HoG) نے گزشتہ دو سال سے تربیت فراہم کرنے کے ساتھ ساتھ گرافک ڈیزائننگ/ملٹی میڈیا میں پیشہ ورانہ خدمات (پروفیشنل سروسز) بھی فراہم کرنا شروع کر دی ہیں۔ یعنی اب جناب عمران شہزاد اور ہاؤس آف گرافکس کی خدمات سے اس میدان میں طالب علموں کے علاوہ پروفیشنل افراد اور ادارے بھی مستفید ہو سکتے ہیں۔

Get your work done before Deadline

With satisfaction what you seek!

Print Solutions



- Logos(2D\3D)
- Books\Magazines
- Flyers\Brochures
- Billboards
- Roll-up-Stands
- Stationary
- Miscellaneous

3D Solutions Architectural



- Walkthroughs
- Interior
- Exterior
- 3D Stalls
- 3D Models
- 3D Animations
- 3D Renders

WEB Solutions



- Static Websites
- Html & Css 3
- Email Ads
- News Letters
- 2D Animations
- Presentations
- Banners Animation

رابطہ

ہاؤس آف گرافکس: 0311-2565660

براہ راست رابطہ عمران شہزاد: 0334-5562974



پی سی ڈاکٹر کے لئے اپنے سوالات editors@computingpk.com پر ارسال کیجیے یا ہمارے فیس بک فین پیج پر بذریعہ ذاتی پیغام ارسال کیجیے۔
کسی پوسٹ پر تبصرے کی صورت میں کئے گئے سوالات پر توجہ نہیں دی جاتی۔کمپیوٹنگ میں صرف چند منتخب سوالات اور ان کے جوابات ہی شائع کئے جاتے ہیں

سوال: کیا ٹورینٹس سے ڈاؤن لوڈ کی گئی فائلوں میں وائرس ہوتے ہیں؟

فہیم احمد، فیس بک

جواب: اس کا مختصر سا جواب ہے "جی ہاں"۔ٹورینٹس سے ڈاؤن لوڈ کی گئی فائلوں میں وائرس کی موجودگی کوئی نئی بات ہے نہ ہی انوکھی۔ پہلے کریک (Crack) کئے گئے سافٹ ویئر ڈاؤن لوڈ کرنے کے لئے فائل شیئرنگ ویب سائٹس استعمال کی جاتی تھیں، اب ان کی جگہ ٹورینٹس ویب سائٹس نے لے لی ہے۔ کئی مقبول فائل شیئرنگ ویب سائٹس کے بند ہوجانے کے بعد ٹورینٹس ویب سائٹس سے سافٹ ویئر، فلمیں، گانے اور دیگر مواد ڈاؤن لوڈ کرنے کے رجحان میں زبردست اضافہ ہوا ہے۔ٹورینٹس ویب سائٹس پر کوئی بھی شخص، دنیا کے کسی بھی کونے میں بیٹھ کر کسی بھی فائل کو ڈاؤن لوڈنگ کے لیے پیش کرسکتا ہے۔ یہ ویب سائٹس پیش کی گئی فائلوں کی کوئی ذمے داری نہیں لیتیں اور نہ ہی انہیں کسی اینٹی وائرس سے اسکین کیا جاتا ہے۔ اس لئے جو فائل آپ نے ٹورینٹ کلائنٹ کی مدد سے ڈاؤن لوڈ کی ہے، اس میں وائرس موجود ہوسکتا ہے۔

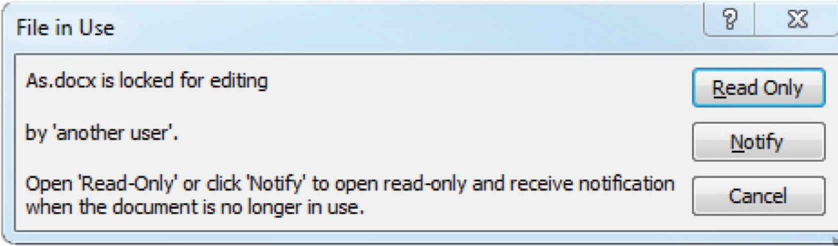
اگر آپ یہ سوچ رہے ہیں کہ آپ تو ٹورینٹس ویب سائٹس سے صرف فلمیں ہی ڈاؤن لوڈ کرتے ہیں اور آپ کو وائرس سے کوئی خطرہ نہیں تو جناب آپ غلط سوچ رہے ہیں۔ یہ بات سب ہی جانتے ہیں کہ exe. یا msi. یا کسی دوسری ایگزی کیوٹ ایبل فائل میں وائرس موجود ہوتا ہے۔لیکن کیا تصاویر اور ویڈیو فائلوں میں بھی وائرس ہوسکتا ہے؟ جی بالکل،ٹورینٹس سے ڈاؤن لوڈ کی گئی ویڈیوز یا تصاویر میں بھی وائرس موجود ہوسکتا ہے۔ البتہ یہ بہت الگ طریقے سے کام کرتے ہیں۔تصاویر اور ویڈیوز چونکہ exe فائلوں کی طرح ایگزی کیوٹ نہیں ہوتیں، اس لئے اگر ان میں وائرس موجود ہو بھی تو براہِ راست چل نہیں پاتا۔ اس لئے ہوشیار قسم کے ہیکر ایک الگ طریقہ کار استعمال کرتے ہیں۔ یہ وائرس کو اس طرح سے تصویر یا ویڈیو کا حصہ بناتے ہیں کہ جب اس تصویر یا ویڈیو کو کسی مخصوص player یا viewer میں کھولا جاتا ہے تو یہ اس پلیئر یا viewer کے اندر موجود کسی خامی کا فائدہ اٹھا کر وائرس والے حصے کو ایگزی کیوٹ کروالیتے ہیں۔ اس طرح سے حملہ آور ہونا مشکل ضرور ہے لیکن ناممکن نہیں۔ ماضی میں ایسے حملوں کی کئی مثالیں موجود ہیں۔

ٹورینٹس سے آپ چاہے کتنی ہی بے ضرر قسم کی فائل ڈاؤن لوڈ کریں یا چاہے کتنی ہی قابلِ بھروسا ویب سائٹ ہو، آپ کو ڈاؤن لوڈ کرنے سے پہلے اس ٹورینٹ پر کئے گئے تبصروں کو ضرور پڑھنا چاہئے۔ اس کے علاوہ فائل ڈاؤن لوڈ کرنے کے بعد اسے چلانے سے پہلے کسی اچھی شہرت کے حامل اینٹی وائرس سے ضرور اسکین کرنا چاہئے اور اینٹی وائرس کو ہمیشہ اپ ڈیٹ رکھنا چاہئے۔ اگر آپ کے کمپیوٹر میں قیمتی ڈیٹا محفوظ ہے تو مفت دستیاب اینٹی وائرس کے بجائے آپ قیمتاً دستیاب اینٹی وائرس استعمال کریں۔ کیونکہ پہلے ڈیٹا وائرس سے متاثرہ ہونے پر اینٹی وائرس سے ٹھیک کرلیا جاتا تھا، لیکن اب جدید وائرس ڈیٹا کو دوبارہ ٹھیک کرنے کے قابل ہی نہیں چھوڑتے۔ ہمارا اشارہ رانسم ویئر کی جانب ہے جو ڈیٹا کو انکرپٹ کردیتے ہیں۔ٹورینٹس ویب سائٹس نے اس خطرے کو دوچند کردیا ہے۔ اس لئے ٹورینٹس ڈاؤن لوڈ کرتے ہوئے بہت احتیاط سے کام لیں۔

سوال: میں نے مائیکروسافٹ ورڈ میں ایک فائل بنائی تھی۔ لیکن اب میں جب بھی اسے کھولنے کی کوشش کرتا ہوں تو مجھے ایک پیغام نظر آتا ہے کہ یہ فائل lock ہے اور اسے کھولا نہیں جاسکتا۔ میں اس فائل کو کیسے دوبارہ کھول سکتا ہوں؟

بخاری، فیس بک

جواب: جب آپ مائیکروسافٹ ورڈ، ایکسل یا پاور پوائنٹ کی کوئی فائل تدوین (editing) کے لئے کھولتے ہیں تو مائیکروسافٹ ورڈ/ ایکسل/ پاور پوائنٹ اس فائل پر ایک خاص قسم کی پابندی لگا دیتا ہے (تکنیکی زبان میں کہیں تو اسے لاک کر دیتا ہے) تا کہ جب تک آپ اس کی تدوین کر رہے ہیں، کوئی دوسرا یوزر اسے کھول کر اس میں کوئی تبدیلی نہ کردے۔ ایسا کرنا حفاظتی نقطہ نظر سے بہت اہم ہے۔ اگر مائیکروسافٹ آفس ایپلی کیشنز ایسا نہ کریں تو آپ کی فائل کو کوئی دوسرا صارف overwrite کرسکتا ہے۔ جب آپ تدوین سے فارغ ہوکر فائل کو بند کرتے ہیں تو آفس ایپلی کیشن فائل پر لگی پابندی بھی ختم کر دیتی ہے۔ لیکن بعض اوقات ایسا نہیں ہو پاتا۔ یعنی فائل بند بھی ہوجاتی ہے لیکن لاک ختم نہیں ہوتا۔ خاص طور پر جب آفس کریش کر جائے یا لیپ ٹاپ/ کمپیوٹر اچانک بند/ ری اسٹارٹ ہوجائے تو ایسی صورت حال پیدا ہوجاتی ہے۔



اس مسئلے کو حل کرنے سے پہلے آپ کو یہ سمجھنا ہوگا کہ مائیکروسافٹ آفس فائل کو لاک کیسے کرتا ہے۔

فرض کریں کہ آپ ایک ورڈ ڈاکیومنٹ abc.docx کھولتے ہیں۔ جیسے ہی مائیکروسافٹ ورڈ اس فائل کو کھولے گا، جس جگہ پر یہ فائل موجود ہے، وہیں ایک نئی فائل abc.docx$~ کے نام سے بن جائے گی۔ آپ نوٹ کیجئے کہ فائل کا نام اصل فائل کے نام جیسا ہی ہے فرق صرف نام کے شروع میں موجود $~ کے نشانات کا ہے۔ یہ فائل پوشیدہ (hidden) ہوتی ہے اس لئے ممکن ہے کہ آپ کو نظر ہی نہ آئے۔ اس فائل کی موجودگی سے آپ abc.docx کے مالک بن جاتے ہیں اور کوئی دوسرا صارف اس فائل کی تدوین نہیں کرسکتا۔ جب تک آپ فائل کو بند نہیں کریں گے، یہ فائل بدستور موجود رہے گی۔ جیسے ہی آپ فائل بند کریں گے یہ فائل خود بخود حذف/ ڈیلیٹ ہوجائے گی۔

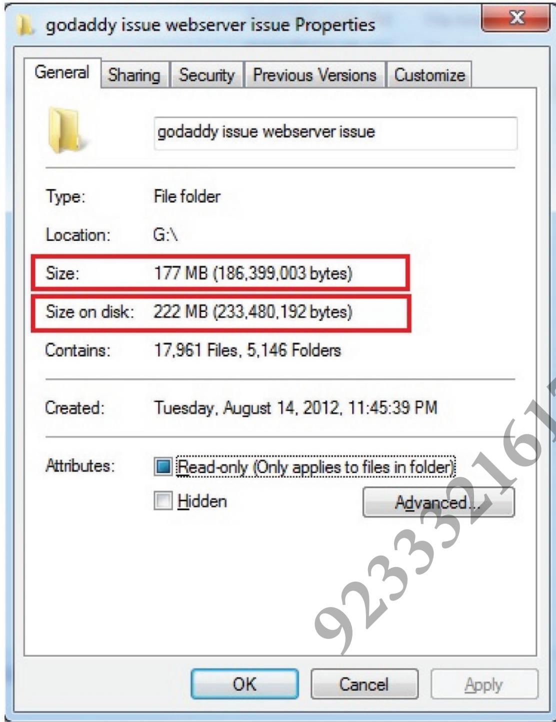
آپ کے کیس میں یہ عارضی لاک فائل ڈیلیٹ نہیں ہو پائی۔ اس لئے آپ جب بھی فائل کھولتے ہیں تو مائیکروسافٹ ورڈ آپ کو فائل کا مالک سمجھنے کے بجائے کوئی دوسرا صارف سمجھتا ہے۔ اس کے کئی حل ہوسکتے ہیں۔ سب سے آسان حل یہ ہے کہ آپ پیغام میں نظر آنے والے Read Only کے بٹن پر کلک کریں۔ اس طرح یہ فائل ناقابلِ تدوین حالت میں کھل جائے گی۔ آپ اس نئی فائل کو Save As کے ذریعے بطور نئی فائل محفوظ کریں۔ یہ نئی فائل کھولنے پر مکمل طور پر قابلِ تدوین ہوگی۔ دوسرا طریقہ جو قدرے مشکل ہوسکتا ہے، یہ ہے کہ آپ اس عارضی فائل کو حذف کردیں یا اس کا نام تبدیل کردیں جس کی وجہ سے فائل لاک ہے۔ جیسا کہ ہم نے پہلے آپ کو بتایا کہ یہ فائل پوشیدہ ہوتی ہے اس لئے یہ آپ کو نظر نہیں آئے گی۔ اسے ظاہر کرنے کے لئے آپ فولڈر آپشن کھولیں۔ فولڈر آپشنز کھولنے کا طریقہ ونڈوز کے مختلف ورژنز میں مختلف ہے۔ ونڈوز سیون میں کسی بھی فولڈر کو کھولیں، کی بورڈ سے ALT کا بٹن دبائیں۔ اس طرح مینو ظاہر ہوجائے گا۔ Tools مینو میں سے Folder Options کا انتخاب کریں۔ ایک طریقہ یہ ہے کہ آپ RUN باکس میں control.exe folders لکھ کر اینٹر کریں۔ فولڈر آپشنز میں View کے ٹیب کھولیں اور پھر Show Hidden files, folders and drives کے ریڈیو بٹن پر کلک کیجئے۔ OK کا بٹن دبائیں۔ اس کے ساتھ ہی آپ کو لاک کا باعث بننے والی عارضی فائل نظر آنا شروع ہوجائے گی۔ اس عارضی فائل کو ڈیلیٹ کرنے سے پہلے اس کا نام تبدیل کریں اور اصل فائل کو کھول کر دیکھیں۔ اگر اصل فائل کامیابی سے کُھل جائے تو پھر آپ اس عارضی فائل جس کا نام آپ نے تبدیل کردیا ہے، ڈیلیٹ کردیں۔

سوال: جب ہم کسی فولڈر یا فائل کی پراپرٹیز کھولتے ہیں تو اس میں دو مختلف سائز نظر آتے ہیں۔ ایک صرف Size ہوتا ہے جبکہ دوسرا Size on Disk۔ ان دونوں میں فرق کیا ہے؟

ریحان، فیس بک

جواب: ایک مثال کے ذریعے ان دونوں کا فرق آپ کو بخوبی سمجھایا جاسکتا ہے۔ فرض کریں کہ آپ کے پاس چار ڈبے ہیں جن میں دو کلو تک کی کوئی چیز ڈالنے کی گنجائش ہے۔ آپ نے ایک ڈبے میں ڈیڑھ کلو چینی ڈالی، دوسرے میں ایک کلو نمک، تیسرے میں دو کلو چاول اور چوتھے میں ایک پاؤ چائے کی پتی۔ اب دیکھا جائے تو ڈبوں میں چیزیں محفوظ کرنے کی مجموعی گنجائش تو آٹھ کلو کی ہے، لیکن آپ نے اس میں صرف پونے پانچ کلو چیزیں محفوظ کی ہیں۔ اس مثال میں ڈبے دراصل کلسٹر سائز یا ایلوکیشن یونٹ ہیں، آٹھ کلو Size on Disk ہے جبکہ پونے پانچ کلو Size ہے۔

Culster ہارڈ ڈسک پر موجود وہ کم سے کم جگہ ہے جسے کسی فائل کو محفوظ کرنے کے لئے استعمال کیا جاسکتا ہے۔ ہارڈ ڈسک پر اس سے کم جگہ کسی فائل کے لئے مخصوص کرنا ممکن نہیں ہوتا۔ اس کا مطلب یہ ہے کہ اگر کلسٹر کا سائز 32 کلو بائٹس ہو اور آپ کی فائل کا سائز صرف 1 کلو بائٹ ہو تو بھی ہارڈ ڈسک پر اس ایک کلو بائٹ کی فائل کے لئے 32 کلو بائٹس کا پورا کلسٹر مخصوص کرنا پڑے گا۔ کلسٹر کے سائز کا انحصار ڈسک کی اپنی گنجائش اور فائل سسٹم پر ہوتا ہے۔ اگر فائل سسٹم FAT16 ہو (چھوٹی گنجائش والے میموری کارڈ کا فائل سسٹم عموماً یہی ہوتا ہے) تو کلسٹر کا سائز 32 کلو بائٹس یا 64 کلو بائٹس ہوسکتا ہے۔ یاد رہے کہ پارٹیشن کو فارمیٹ کرتے ہوئے آپ کلسٹر کا سائز بھی منتخب کرسکتے ہیں۔ NTFS فائل سسٹم میں کلسٹر کا سائز 4 کلو بائٹ ہوتا ہے۔



فرض کیجئے کہ پارٹیشن کا فائل سسٹم NTFS ہے اور ایک فولڈر میں آپ نے ایک کلو بائٹ کی 4000 فائلیں محفوظ کررکھی ہیں۔ تو اگرچہ اس فولڈر کا اصل سائز 4000 کلو بائٹ یا 4 میگا بائٹس ہوگا۔ لیکن چونکہ کلسٹر کا سائز 4 کلو بائٹس ہے اور ہر فائل کے لئے الگ کلسٹر مخصوص کرنا ضروری ہے، اس لئے ان چار ہزار فائلوں کو محفوظ کرنے کے لئے چار ہزار کلسٹر مخصوص کرنے ہونگے جن کا مجموعی سائز 16000 کلو بائٹ یا 16 میگا بائٹس ہوگا۔ اسے ہم Size on Disk کہیں گے۔ اب کچھ دیر کے لئے فرض کیجئے کہ کلسٹر کا سائز 4 کلو بائٹس نہیں بلکہ 32 کلو بائٹس ہے۔ اس صورت میں ایک کلو بائٹ کی چار ہزار فائلیں ڈسک پر 128 میگا بائٹس کی جگہ پر قبضہ کئے بیٹھی ہونگی۔

کلسٹر سائز اگر بڑا ہو اور انفرادی فائلوں کا سائز چھوٹا ہو تو ڈِسک کا ایک بڑا حصہ ضائع ہوجاتا ہے۔ اس لئے اگر آپ کو پتا ہو کہ جو فائلیں آپ محفوظ کرنے جارہے ہیں، وہ بہت چھوٹے سائز کی ہیں تو پارٹیشن کو فارمیٹ کرتے ہوئے ایلوکیشن سائز یونٹ/کلسٹر کا سائز کم سے کم منتخب کریں۔ لیکن اگر آپ نے ڈِسک میں صرف بڑی فائلیں مثلاً فلمیں محفوظ کرنی ہیں جن کا سائز کئی سو میگا بائٹس یا گیگا بائٹس ہوتا ہے تو ڈِسک کو فارمیٹ کرتے ہوئے کلسٹر سائز بڑا منتخب کرنا چاہئے۔ جہاں آپ کو اندازہ نہ ہو کہ فائلیں چھوٹی ہوں گی یا بڑی، وہاں کلسٹر سائز کو تبدیل کرنے کی ضرورت نہیں۔

عام استعمال کے لئے NTFS فائل سسٹم بہترین ہے کیونکہ اس میں کلسٹر کا سائز 4 کلو بائٹس ہے۔ لیکن میموری کارڈ کو NTFS فائل سسٹم پر منتقل کرنا مناسب عمل نہیں۔ اس لئے میموری کارڈ کو FAT32 فائل سسٹم کے لئے فارمیٹ کرنا چاہئے۔

سوال: میرے گوگل کروم میں ایڈ ویئر داخل ہوگیا ہے اور اب حالت یہ ہے کہ میں بے تحاشہ اشتہارات کی بھر مار میں اُلجھ سا گیا ہوں۔ میں نے پہلے گوگل کروم نئے سرے سے انسٹال کیا پھر ایک سافٹ ویئر ADW Cleaner استعمال کیا، مگر مسئلہ جوں کا توں رہا۔ اب آپ ہی میری مدد کیجیے۔

(محمد کاشف، ای میل)

جواب: سب سے پہلے آپ کو وہ تمام ٹول بارز اور نامعلوم قسم کے اینٹی وائرس اپنے کمپیوٹر سے اَن انسٹال کردینے چاہئے جن کے بارے میں آپ کو ذرا سا بھی شبہ ہے کہ وہ آپ نے خود انسٹال نہیں کئے یا وہ آپ کے کام کے نہیں۔ جب آپ انٹرنیٹ سے کوئی سافٹ ویئر ڈاؤن لوڈ کرتے ہیں تو اس بات کی یقین دہانی کرلیا کریں کہ وہ سافٹ ویئر کسی ایڈ ویئر سے پاک ہے۔ اس کے لئے ہمیشہ کسی معروف اور قابلِ بھروسا ویب سائٹ مثلاً www.downloads.com یا sf.net سے سافٹ ویئر ڈاؤن لوڈ کریں۔

اگر آپ انٹرنیٹ سے غیر ضروری سافٹ ویئر ڈاؤن لوڈ کرکے انسٹال کرنے کے عادی ہیں تو یاد رکھیں، یہی سافٹ ویئر آپ کے کمپیوٹر میں ایڈ ویئر کی آمد کا باعث بنتے ہیں۔ فائل شیئرنگ ویب سائٹس سے فائلیں ڈاؤن لوڈ کرنے کی کوشش میں بھی کئی لوگ اپنے کمپیوٹر میں خطرناک سافٹ ویئر انسٹال کر بیٹھتے ہیں۔ ان سافٹ ویئر کے ساتھ خفیہ طور پر ایڈ ویئر بھی موجود ہوتا ہے یا یہ دوران استعمال اسے انٹرنیٹ سے ڈاؤن لوڈ کرلیتے ہیں۔ جب بھی آپ کوئی پروگرام انسٹال کریں تو انسٹالیشن وزارڈ کے دوران اپنی آنکھیں کُھلی رکھیں کہ یہ سافٹ ویئر کہیں مزید کوئی پروگرام یا ٹول بار تو انسٹال نہیں کررہا۔ ہمارے تجربے کے مطابق زیادہ تر متاثرہ کمپیوٹرز میں ایڈ ویئر ٹول بارز صارف کی لاپروائی سے انسٹال ہوتی ہیں۔

گوگل کروم میں اشتہارات کا باعث بننے والا ایڈ ویئر بھی اسی طرح آپ کے کمپیوٹر میں داخل ہوا ہے۔ اسے ختم کرنے کے لئے آپ گوگل کروم کو کھولیں اور ایڈریس بار کے دائیں جانب موجود "پانے" کے یا تین سطروں کے نشان پر کلک کریں۔ ایک ڈراپ ڈاؤن مینو ظاہر ہوگا۔ اس ڈراپ ڈاؤن مینو میں سے Settings کا آپشن منتخب کریں۔ سیٹنگز کی ونڈو گوگل کروم کے ایک ٹیب ہی میں کھل جائے گی۔ اس میں بائیں جانب Extensions کا آپشن تلاش کیجئے اور اس پر کلک کردیں۔ آپ ایکسٹینشنز کا پیج ایڈریس بار میں درج ذیل کمانڈ ٹائپ کرکے بھی کھول سکتے ہیں:

chrome://extensions/

آپ کے سامنے ان تمام ایکسٹینشنز کی فہرست کھل جائے گی جو کہ فعال یا غیر فعال ہیں۔ آپ اس فہرست کا اچھی طرح جائزہ لیں تو دیکھیں کہ ان میں سے کون سے ایکسٹینشن ایسے ہیں جنہیں آپ نے انسٹال نہیں کیا یا وہ آپ کے لئے انجان ہیں یا پھر آپ کے کام کے ہی نہیں۔ ایسے تمام غیر ضروری ایکسٹینشنز کو فی الفور غیر فعال یا disable کردیں۔ اس کے لئے ان کے نام کے سامنے موجود enable کے چیک باکس کو اَن چیک (uncheck) کردیں یا انہیں سرے سے ڈیلیٹ ہی کرنے کے لئے یہیں موجود ری سائیکل بن کے آئی کن پر کلک کردیں۔ اس کام سے فارغ ہوکر گوگل کروم کو ری اسٹارٹ کرلیں۔ قوی امکان ہے کہ اشتہارات سے آپ کی جان چھوٹ جائے گی۔



پاکستان بھر میں کمپیوٹنگ کے ڈسٹری بیوٹرز



شہر	ڈسٹری بیوٹر
کراچی	گلستان نیوز ایجنسی، فریئر مارکیٹ
راولپنڈی	اشرف نیوز ایجنسی، کمیٹی چوک، اقبال روڈ
لاہور	گلزار نیوز ایجنسی، اخبار مارکیٹ
پشاور	اطلس نیوز ایجنسی، بشیر چیمبر، مسجد مہابت خان روڈ
رحیم یار خان	چوہدری امانت علی اینڈ سنز
حیدر آباد	مہران نیوز ایجنسی

* **احمد پور ایسٹ:** اسلامی کتب خانہ، نزد گرلز ہائی اسکول، ڈسٹرکٹ بہاول پور
* **احمد پور شرقیہ:** اسلامی کتب خانہ، ضلع بہاولپور
* **اوکاڑہ:** رحمت بک اسٹال، نزد ریلوے پل
* **بنوں:** امیر جان نیوز ایجنسی، چوک بازار، ضلع بنوں
* **بہاولنگر:** دولت خان نیوز ایجنسی، اردو بازار، بہاولنگر
* **تلہ گنگ:** گلوبل کمپیوٹر سینٹر، اولڈ بس اسٹینڈ، ڈسٹرکٹ چکوال
* **تربت:** پاک نیوز ایجنسی، مین روڈ
* **جھنگ:** شیخ محمد حسین نیوز ایجنٹ، فوارہ چوک، جھنگ صدر
* **جھنگ:** ہمدرد نیوز ایجنسی، رفیقی چوک، شورکوٹ چھاؤنی
* **چشتیاں:** شاہین لائبریری، اُردو بازار، ضلع بہاولنگر
* **چشتیاں:** دولت خان نیوز ایجنسی، اردو بازار
* **حاصل پور:** محمد وقاص وحید نیوز ایجنسی، ضلع بہاولپور
* **خانپور:** چوہدری بشیر امانت علی اینڈ برادرز، ریلوے روڈ
* **خانیوال:** طاہر اسٹیشنری مارٹ اینڈ نیوز ایجنسی، کچہری بازار
* **ڈیرہ اسماعیل خان:** قمر بک اسٹال، اردو بازار
* **ڈیرہ غازی خان:** ناصر نیوز ایجنسی، فریدی بازار، ٹریفک چوک
* **ساہیوال:** زمیندار نیوز ایجنسی، چوک صدر، لاہور
* **سرگودھا:** پاکستان اسٹینڈرڈ بک ڈپو، بلاک نمبر 10، پھٹہ منڈی روڈ
* **سرگودھا:** پاکستان نیوز ایجنسی، نزد گول چوک، پھٹہ منڈی روڈ
* **سکھر:** الفتح نیوز ایجنسی، مہران مرکز
* **سیالکوٹ:** علمی مرکز، اردو بازار
* **صادق آباد:** چوہدری نیوز ایجنسی، ریلوے روڈ
* **کوٹ ادو:** عابد شاہ پرفروش، بالمقابل بس اسٹینڈ، کوٹ ادو، ضلع مظفر گڑھ
* **گجرات:** پاکستان بک سروس، 30، اُردو بازار
* **گجرات:** خالد بک ڈپو، مسلم بازار
* **گلگت:** نارتھ بکس، مدینہ سپر مارکیٹ
* **مظفر گڑھ:** محمد عبدالطیف بلوچ نیشنل نیوز ایجنسی، قنوان چوک
* **میانوالی:** محمدی نیوز ایجنسی، لاری اڈہ
* **واہ کینٹ:** خوشبو ڈائجسٹ سینٹر اینڈ لائبریری، نواب آباد
* **واہ کینٹ:** حبیب اللہ قمر، میلاد چوک
* **وزیر آباد:** نوید نیوز ایجنسی، ریلوے بکسٹال

اگر کمپیوٹنگ آپ کے علاقے میں دستیاب نہیں تو برائے مہربانی ہمیں اس نمبر پر مطلع فرمائیں:

0342-2507857

DON'T TAKE THE BAIT

IF IN DOUBT, GET IT CHECKED OUT



UHU®

stic

glue stick

The exclusive screw cap prevents the glue from drying.



UHU the world of Adhesives